* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
(Background of invention)
1. Field of invention Generally this invention relates to cybermoney, an electronic ticket, an electronic coupon, an electronic check, a digital ticket, etc.
[0002]
Are efficiently [cheaply and] producible. this invention -- especially -- (i) insurance and quickness -- the digital communication network in the world -- leading -- distribution -- possible -- (ii) -- it can inspect visually by the purchase addressee, and it is physically safe, can convey, and is strong to fabrication (iii) -- namely, effect -- not winning popularity (however) A network invader, the purchase addressee of each digital ticket, and/or the purchase addressee of a large number which participate in conspiracy If a certain (iv) purchase addressee desires possibility of fabricating such a digital ticket Purchase anonymously, hold, can return and are based on laser scanning of a (v)2-D bar code format. Popularity is won including being based from a smart card on data reading etc. or easily at the time of return Quickly, can verify safely and not a winning popularity return is allowed after (vi) duplex receptacle return or a report of all thefts (resistant). It has the versatility incorporating various ratings. (vii) a move and division -- possible -- self-(viii) authentication -- carrying out -- (ix) -- (x) That cancellation is possible or winning popularity return is possible, and it is related with a digital ticket healthy on (xi) ecology target. [be / no physical liquidation (tender) or physical cancellation (surrender)]
[0003]
2. Explanation 2.1 of conventional technique General background 2.1.1 General preface The amount of the electronic commerce (electronic commerce) in both transaction (transaction) between firms and between firm-consumers is increasing dramatically in recent years. Almost all consumers' Internet commercial transaction is due to processing by the credit card, and is U.S.Postal Service. United Parcel Service Federal Express Or goods are sent to the consumer using general parcel delivery service like Airborne Express. Although it is completely rational about physical goods, such as books, Music CD and DVD, or same goods, it is thought that use of the physical delivery for the purchase of an abstract concept like an access privilege is unsuitable.
[0004]
What kind of access privilege is sold on the Internet? It will be movie Star Wars early in May, 1999. : The Phantom Menace A ticket becomes available on in TANETSU, and it could purchase with the credit card before rather than it was sold by the box office of a movie theater. This is far attractive alternative rather than it makes a matrix and stands in a line in advance of public presentation of a popular movie. Theater, ballet, a concert, and a sport event are contained in the access privilege of other classes currently sold on the Internet.
[0005]
In case the ticket of a movie is purchased on the Internet now, a consumer has to acquire a ticket

physically, therefore this has functioning [more] as a reservation device in a sense. Like the ticket of theater or a sport event, if the value and the price of a ticket become high, a ticket will be delivered by the consumer by mail in many cases.
[0006]
A ticket is a physical body showing the access privilege of single use. Instead of mailing, the artificer of this invention distributes such an access privilege electronically with the gestalt of a digital ticket, and it is sure that he is natural. Since the digital representation of the right contained in a ticket must be [in / an access point] verifiable with the ticket ticket collector of a theater, as for a ticket, it is desirable for it to be able to change into the gestalt which can be conveyed easily physically. In order to perform authentication and verification, digital ticket contents can be again digitized from the gestalt printed without spending costs easily when reading was possible and it was required, and should contain an authentication tag like a digital signature. The digital data inside a digital ticket can be carried to the venue of a ticket event by various approaches by the consumer. Store digital data in a flexible disk, it is stored in a smart card, or can perform printing in the paper etc.
[0007]
Use of the printed two dimensions bar code is considered to be desirable by the artificer of this invention as an encoding technique for which it was very suitable for digital ticket purchase. ItKin and Josephine Martell; A PDF417 primer: A guide to understanding second generation bar codes and portable data files; Refer to Technical Report Monograph 8 and Symbol Technologies (April, 1992). Moreover, AIM Also refer to specification"Uniform Symbology Specification PDF147." The printed 2-D bar code is excellent in the fault tolerance nature of the held data, and re-digitization is easy for it. Thus, economical initial commercial-scene osmosis is possible for the printed digital ticket, and if a compromise is reached in some gestalten of a ticket, and user-friendliness of contents, the hardware foundation structure of the consumer who exists at hand can be used. That is, unlike the situation of smart card reader/writer, many web surfers can access a printer.
[0008]
2.1.2 Requirements for Internet ticket issue It can also be considered that the Internet ticket is the digital representation of an access privilege or capability (capability). These can be consumed at the time of use, or can be confirmed over a certain time amount period. For example, it is the relation of the ticket of a movie, and the series ticket of film series. Furthermore, generally such a ticket can prepare constraint in the use. For example, a lecture has effective movie pass only 5 times in the morning.
[0009]
Unlike the capability in the conventional capability orientation mold operating system, the capability of a digital ticket is not maintained by the kernel of an operating system which performs transmission and reading of a ticket. The probably nearest prototype is use of the Amoeba distribution kernel of capability, and capability transmits through a network in this case. editor of Sape J.Mullernder ; The Amoeba distributed operating system: Selected papers 1984-1987; Refer to Centre for Mathematics and Computer Science and 1987. However, in the case of an Internet digital ticket, finally, a consumer carries the generated digital ticket through a "SUNEKA network" (sneaker net) to a movie theater or a concert venue.
[0010]
It is good to compare with other two electronic commerce methods, the cybermoney, and digital mail which have the requirements which were very alike in part in consideration of the functional requirements over the Internet ticket. However, depending on a difference of requirements, digital designs may completely differ. The following chapters 2.1.3 and 2.1.4 consider cybermoney and digital postal-charge sealing.
[0011]
2.1.3 Cybermoney Cybermoney is in the electronic commerce method which has many of same requirements as a digital ticket. The electronic expression of money has worth of a proper with a certain gestalt completely like a digital ticket. T. Okamoto and K.Ohta; Universal electroniccash in Advances in Cryptology -- Refer to listing and explanation of functional requirements in Crypto'91, pages 324-

337;Springer-Verlag, and 1992 which were excellent in cybermoney.
[0012]
Okamoto and Ohta are summarized as follows as requirements.
(1) The independence for which the safety of electronic cash does not depend on a certain physical device.
(2) Safety which electronic cash cannot create except an issuing bank. Fabrication must be easily detectable. Detection being possible and a trace must be possible for duplex receptacle return.
(3) Privacy to which proper use of cybermoney does not expose a consumer's identity.
(4) Off-line-processing possibility that pay, and processing does not need network access and does not need a break in of a third person.
(5) Transferability which can transfer cybermoney among customers.
(6) Division possibility which can do exchange easily.
[0013]
2.1.4 Sealing based on information [as / in an electronic stamp] (IBI) Sealing based on information gives the one approach of showing having paid the postage on an envelope. U. S.Postal Service; Refer to Information Based Indicia Program (IBIP) New Technology Metering Devices (May, 1995). The two dimensions bar code (PDF417) which encoded the digital signature for this purpose is used for IBI specification. U. S.Postal Service; Refer to Information Based Indicia Program (IBIP) Indicia Specification (July, 1996). Moreover, Stuart Itkin and Josephine Martell; A PDF417 primer: A guide to understanding second generation bar codes and portable data files; Also refer to Technical Report Monograph 8 and Symbol Technologies (April, 1992).
[0014]
Although the application of a digital postal charge is similar to the Internet circulation digital ticket, it has caused complication of a solution for the requirement. Here, although the effectiveness of sealing must be judged, a digital signature must be verified, it must collate with a master database and a duplicate must be prevented, it depends for such duplicate use detection on a distributed database. Furthermore, since worth of a stamp is low, depending on the case, it has suggested that the direction of only the very cheap cure against fraud detection is cost-performance-like. Moreover, **** must be able to be printed off-line completely and the need for the communication link in a post office must be able to be controlled. For this reason, a mail security device (PSD) will be used. This is a special secure co-processor, even when PSD is in a hostile environment potentially, maintains a balance and offers the safe method of performing code count.
[0015]
Unlike sealing, usually, in a certain physical location which the ticket like a movie theater, a concert hall, and a sport arena itself shows, for example, a ticket is made into a target and "is consumed." This simplifies the work which detects a duplicate. It is because the need for network construction is localized rather than the case of postal-charge sealing. The much more elaborate cure against fraud detection is attained at it, so that worth of a ticket is high to coincidence. The interactive property of ticket purchase processing required for both statement maintenance of a reserved seat (assigned-seating) ticket and a quantity sold can raise the flexibility of a system design.
[0016]
2.1.5 Internet ticket Many of functional requirements over cybermoney do not change a ticket, either. Almost all tickets are those (consume) which disappears when used, and division possibility does not serve as important requirements. In the case of pass or a concert series ticket, just a simple expiration date is enough.
[0017]
Ticket It must be able to distribute on-line [(1)]. Using a standard web tool like the web browser corresponding to SSL, a user has to purchase a ticket and has to receive the distribution.
(2) It must be insurance. A ticket cannot be created except a publishing agency, but fabrication can be detected easily, and a detectable /trace is possible for winning popularity return of a duplex.
(3) It must be a secret. Proper use of a ticket does not necessarily expose an identity. (This is not the

property of Ticketmaster (trademark) or Will Call (trademark) in current.) In order to receive a ticket, it is because discernment is required.
[0018]
The requirements for online distribution simplify many fields of a design. Since a ticket publishing office must maintain the database of the sold ticket to a seat assignment ticket and the number of tickets of a general entrance ticket must be maintained at worst, the design which is not completely online is also allowed. There may also be superfluous reservation, and for an application like an aircraft ticket, although it is general, the number of superfluous reservation must still be restricted and managed. It is because superfluous reservation is not economically healthy.
[0019]
2.2 Concrete background 2.2.1 Security to the end user who accesses a web server To the conventional technique which is related to this invention, they are Axent Techonologies of California Mountain View, and Inc. There are the system and product which strengthen the security of the end user who accesses the web server of ["Axent"]. this technique -- very much -- relation -- it is because a server can publish a digital ticket to a customer if a server can identify a customer safely and deep one is [1st] possible also for that reverse.
[0020]
However, the still more important comparing point is much more delicate. This invention notes enciphering much the amounts of data or the fields in an certain aspect of affairs (juncture). With the following paragraph [4th], the amount of encryption and a "message authorization code" show clearly that they are some digital tickets in an Axent system.
[0021]
In generation and circulation of an encryption ticket, since Axent gives protection with the proper "Web Defender" server software, the user could log in to the web server of a large number over between companies, and has said that it does not need to enter an additional password each time.
[0022]
Furthermore, since it is required that Web Defender should provide a networker with the approach of pursuing and managing these tickets intensively, a good thing is the name of an individual or a group, and can control access to company data. It is not necessary to correct a customer's browser during a setup.
[0023]
Web Defender lurks behind the fire wall of a company, and performs collaboration with the web server which runs Internet Information Server (IIS) from Microsoft Corporation (Redmond, Washington). this -- Microsoft from -- it operates with both Communicator from Internet Explorer and Netscape Communications Corporation (Mountain View, California).
[0024]
In the setup of Web Defender, the 1st step is acquiring the digital certificate of attestation for an IIS web server from a third party certificate station like Verisign and Incorporated (Mountain View, California). This enables a web server to start a SSL (secure sockets layer) session using a web browser. Next, a network manager chooses NT domain and the group to whom access to a Web Defender server is permitted (minding GUI). A group is chosen from NT domain and, subsequently cut and paste is performed within Web Defender. It is only only choosing a general ticket issue property, such as making a message send to a web browser, once a sign-on process's is successful after that, or carrying out the recurrence line of the ticket automatically, once an old ticket's expires.
[0025]
Then, Web Defender software "raises" (pump up) security how. A user acts [1st] as key Inn of the name and password which received authentication by the Web Defender server. (It is important to touch on that a password and a user's name are on SSL connection, and are exchanged only once during this initial authentication) . To the 2nd, a Web Defender server creates a user ticket including some data fields like a user's identifier, the shelf-life of a ticket, and a group name. These all specify the data which a ticket holder may access. A ticket is applied for the MD5 encryption algorithm which RSA Data

Security Incorporated (Redwood City, California) developed, and a message authorization code is generated [3rd]. This becomes a part of ticket itself. At this time, a digital ticket is published and it stores in the memory of a user's web browser. Once a session is completed, a ticket will be deleted from memory.

[0026]

2.2.2 Former patent A series of patents of Stefik transferred to Xerox Corporation (Stamford, Connecticut) and et al. treat the distribution and use containing a digital ticket (not necessarily limited to this) of a valuable digital work piece (work). U.S. Pat. No. 5,715,403 SYSTEM FOR CONTROLLING THE DISTRIBUTION AND USE OF DIGITAL WORKS HAVING ATTACHED USAGE RIGHTS WHERE THE USAGE RIGHTS ARE DEFINED BY A USAGE RIGHTS GRAMMAR (a royalty) It is given to the system which controls the distribution and use of a digital work piece to which the royalty was attached when specifying according to royalty syntax. U.S. Pat. No. 5,638,443 It is given to a SYSTEM FOR CONTROLLING THE DISTRIBUTION AND USE OF COMPOSITE DIGITAL WORKS (system which controls distribution and use of a decode digital work piece). U.S. Pat. No. 5,634,012 a SYSTEM FOR CONTROLLING THE DISTRIBUTION AND USE OF DIGITAL WORKS HAVING A FEE REPORTING MECHANISM (a tariff report device) It is given to the system which controls the distribution and use of a digital work piece which it has. And U.S. Pat. No. 5,629,980 It is given to a SYSTEM FOR CONTROLLING THE DISTRIBUTION AND USE OF DIGITAL WORKS (system which controls distribution and use of a digital work piece). The application 08th entitled "SYSTEM FOR CONTROLLING THE DISTRIBUTION AND USE OF DIGITAL WORKS USING DIGITAL TICKETS" (system which controls distribution and use of the digital work piece using a digital ticket) which shall be first contained also in this application / No. 344,760 are not published as a patent yet.

[0027]

These patents have relation in this invention about the property of the security of the system which mainly communicates through a network top and this as a background specifically. a direct confrontation object [in / in use of the "reliance repository" (trusted repositories) in these patents / the fundamental system of this invention] -- being out of range . However, this invention does not have **** which is adopted and developed worldwide and is used for billions of ticket issue every month, and it does not necessarily come from the issue origin with all the same tickets even about the same event. Therefore, the patent of Xerox shows how the digital ticket issue system and approach of this invention are expandable to infinity.

[0028]

All of these patents are related with the system which controls use and distribution of a digital work piece. This system makes a royalty accompany the owner of a digital work piece at the work piece of his or her. A royalty specifies how I may make each digital work piece use and distribute. The example of a royalty is specified using flexible and extensible royalty guidance. Notionally, the right in royalty guidance is the label which associated the predetermined behavior and the predetermined conditions over the exercise. The behavior of a royalty is materialized in 1 set of predetermined use transaction processes. Furthermore, a use transaction process checks all the conditions that must be fulfilled before the exercise becomes possible. These use transaction processes require the exercise and specify the protocol for performing a right.

[0029]

Therefore, the above-mentioned patent is related to the field of the distribution to the work piece encoded in digital one, and royalty use. These are inaccurate, and in preventing the distribution and use of an electronic publishing material which explanation does not attach, they are dealing with the fundamental problem currently faced with publication and the information industry. Including various things, usually, an electronic publishing material is distributed with a digital gestalt, and is reproduced on the computer system which can reproduce this material. Although these patents have extracted an audio and video record, software, books, and a multimedia work piece as an example of electronic publishing, they can consider that a digital ticket is also an electronic publishing work piece, and are

actually the electronic publishing work pieces of a value fluctuation mold at least.
[0030]
The patent of Xerox is tackling the problem of safe distribution of the digital work piece by use of a reliance repository. The thing in which many of powerful functions of a repository like capacity which "lends" the digital work piece, or treats commercial reuse of a digital work piece automatically are possible is because these are reliance systems. the system is trusted -- these -- a commercial transaction -- fair -- and dependability -- it is because the responsibility carried out highly can be taken. It is the problem of integrity fundamentally that a system can take responsibility ("it can answer"). The integrity of a repository has three parts, physical integrity, and communications security nature and behavior-integrity.
[0031]
Physical integrity means the integrity of the physical device itself. Physical integrity is applied to both digital work piece a repository and for protection. Therefore, these very thing may have the sensor which detects the repository of a high security class when an alteration tends to be performed on those insurance cases. In addition to protection of the repository itself, the design of a repository also protects access to the contents of a digital work piece. An unreliable system is not made to never carry out direct access of the repository to a work piece in contrast with the design of the conventional MAG and the optical device like a floppy disk, CD-ROM, and a video tape. The manufacturer of a general purpose computer system cannot guarantee that an illegal copy is not created using their platform. A manufacturer offers the general function which reads information and writes in, and it depends for the synthetic property of the functionality of a general-purpose computer on it. Therefore, a copy program can copy the data of arbitration. This copy problem is not necessarily restricted to a general purpose computer. This is generated also about an unjust duplicate for amusement "software" like the video by the magnetic recording medium, and audio record. These do not have a means to confirm whether, as for the functionality of a recording apparatus, the copy is permitted also in this case depending on that copy capacity. By contrast, a repository can prevent access to the raw data based on a general-purpose device, and can inspect a copy, and a right and conditions explicit before the other access grant. Only between reliance repositories, information is accessed with a protocol.
[0032]
Communications security nature means the integrity of the communication channel between repositories. If it says roughly, communications security nature means that a repository cannot be easily deceived by what "a lie is told for." The integrity in this case means the thing of a property which it communicates with these only when the certification of other devices being the attested repositories can be submitted, and a repository supervises a communication link, and detects a "swindler" and malice, or an accidental interference. Therefore, all the security countermeasures containing encryption, exchange of a digital certificate of attestation, and the nuance (nuance) described below are security countermeasures aiming at the high-reliability communication link in the world where it turns out that there is an actual adversary.
[0033]
Behavior-integrity is the integrity in performing a repository. The software which these perform decides that a repository carries out. Generally the integrity of software is guaranteed only by the knowledge of the source. In other words, although a user trusts the software purchased in the reputable computer dealer, he does not trust the software acquired from the random (it is not safe) server on a network. In order to maintain behavior-integrity, repository software has received authentication and must make it distribute with the certification of such a certificate of attestation, i.e., a digital certificate of attestation. It proves that the purpose of a certificate of attestation is attesting it being inspection ending by the official-recognition engine, and software performs that it is assumed that it performs software and does not spoil the behavior dependability of a repository. Software cannot be installed when the master repository which a digital certificate of attestation could not find it within the digital work piece, or generated the certificate of attestation is not known by the repository which accepted software.
[0034]

All repositories offer 1 set of core services for transmission of a digital work piece. The method of exchanging a digital work piece is the base of all the transactions between repositories. The final function which these perform in the form of various repositories has a difference. A repository may be these the very thing device, or you may also include it in an alien system.
[0035]
The repository identifier is related with the repository. Usually, a repository identifier is the number of the meaning assigned to a repository at the time of manufacture. Moreover, each repository is classified as a thing belonging to a specific security class. A certain kind of a communication link and a transaction may be subject [to a repository belonging to a specific security class]. As a prerequisite of operation, a repository needs possession of a discernment certificate of attestation. A discernment certificate of attestation is enciphered, an alteration is prevented, and a master repository publishes this. A master repository plays an official-recognition agent's role, and enables a repository to receive a digital work piece. A discernment certificate of attestation must be updated periodically. A discernment certificate of attestation is explained in more detail below about a registration transaction.
[0036]
A repository has both hardware and a functional operation gestalt. A functional operation gestalt is software performed on a hardware operation gestalt in usually. Or a functional operation gestalt can also take shape in a hardware operation gestalt like a specified use integrated-circuit (ASIC) chip.
[0037]
The hardware operation gestalt of a repository is sealed in safe housing, and when exposed to risk, it can carry out the disable of the repository. The fundamental component of the hardware operation gestalt of a repository contains a processing means, a storage system, a clock, and an external interface.
[0038]
Core repository service consists of 1 set of functions which each repository needs. Core repository service includes a session initiation transaction. The comprehensive ticket agent who uses in case a digital ticket "is punched", and the comprehensive official-recognition server which processes official-recognition assignment (authorization specification) also include 1 set of these services. A digital ticket and official recognition are concrete devices which control distribution and use of a digital work piece. In addition, combining with core repository service describes that they are two or more discernment certificates of attestation. In order to enable use of a repository, a discernment certificate of attestation is needed.
[0039]
The deformation (variant) on this method about a royalty is having a digital ticket apparently. A digital ticket agent is shown a ticket and the class is specified on a ticket. But when simple, an attested all-inclusive ticket agent available on all repositories "can punch" a ticket. In other cases, a ticket can include the addressing information for tracing a "special" ticket agent. Once it punches a ticket, it cannot be again used for the transaction of the same class (unless it restores punching so that it may state below, i.e., it refreshes). Punching includes inscribing the time stump of the time which the ticket used on a ticket. A ticket is a digital work piece, and according to the royalty, it can copy between repositories or it can be transferred.
[0040]
With a suitable operation gestalt at present, the ticket "punched" punched ["un-punching"] namely, "will be refreshed", when it copies or extracts. A copy and extract actuation save time as a property of a digital ticket. If a ticket is given to a ticket agent, a digital copy can confirm clearly whether it was made after it was punched at the end. Of course, the copy or the extract royalty must accompany the digital ticket.
[0041]
The capability [-izing / a ticket / capability / un-punching] becomes important in the following cases.
(1) Circulate this by low cost with [that a digital work piece can be used only at once] a limit.
[0042]
(2) A digital work piece is circulated with a ticket usable once, and discount is obtained at the time of

the purchase of other work pieces.
(3) Circulate a digital work piece to a future upgrade with an usable ticket (it is contained in a purchase price and, probably embedded to the work piece).
[0043]
In each in these cases, probably a new owner is not concerned with whether the vender of a copy used the work piece, but expects that an intact ticket (un-punching) will be obtained, when the paid copy is made from the digital work piece (a ticket is included). A ticket should not be revived, when by contrast lending a work piece or only transferring it to other repositories.
[0044]
2.2.3 Framework of general-purpose digital ticket Ko Fujimura and Yoshiaki Nakjima of NTT Information and Communication Systems Labs are tackling the digital ticket. Mr. Fujimura has worked out a detailed plan for the flexible digital ticket which makes it a key objective to develop the comprehensive value circulation medium which prevents duplex use. In this context, a ticket is a digital medium which guarantees the right which the owner of the ticket concerned has. Generally by description of a ticket, it becomes possible for a ticket to include the value that a large number differ in a single ticket (or the group), and different worth of a class.
[0045]
Mr. Fujimura claims that a general-purpose ticket framework reduces operation cost in many cases. It is because a single design can be used in many locations. By becoming common, a ticket can be constituted in arbitration and bundling (bundling) and the same feature (feature) can be made possible. It is claimed that creation of the new business in which he realizes this framework like issue/discharge service or deposit box service (deposit box service) was effective.
[0046]
A general-purpose digital ticket framework must satisfy most requirements for a digital cash. There are the following in additional requirements. (1) A ticket can control the anonymity, division possibility, and transferability according to an application. (2) "The machine understanding of each specification of a ticket is enabled", and make possible winning popularity return of a product or service. (3) The ticket property (for example, paying or reservation status) with which value changes while circulating must be changed to insurance. (4) It must correspond to the ticket which consists of more subtickets than one.
[0047]
In order to carry out such a framework, the author created the ticket definition language which enables assignment of a ticket property. The ticket itself makes possible automation of a state transition, and a compound possibility feature on the basis of a hypertext. Moreover, a ticket can also include the dynamic information which will be updated if the ticket itself is used. As another (obvious availability is low) feature, an image and very big data like a sound can be included in a ticket.
[0048]
Although the ticket itself is originally online (being based on the hypertext, and a dynamic property sake), it is possible to also make it circulate off-line using a smart card. In any case, a system inspects the currency (currency) of a ticket using URI which signed. The semantics of a property and constraint in a ticket are specified using a resource description framework. Therefore, the framework to a ticket can be controlled by the publisher of a ticket, and can include various constraint in these frameworks.
[0049]
Fujimura explained the outline of a ticket reliance model. A publisher's certificate of attestation, a user's certificate of attestation, and an inspector's certificate of attestation are required for issue, transition, consumption, or inspection of a ticket, and are specified to the ticket itself using ticket definition language. Therefore, each ticket equipped with the public key like a driver's license document can be used as a public key certificate of attestation, if a ticket specifies them as a certificate of attestation required for a ticket. In other words, all tickets can play a role in the public key foundation structure of other tickets.
[0050]
Fujimura and Nakajima plan to draft the operation detail and to submit them to a standard engine. The

target of their project is what "all web terminals are changed into a ticket issue machine for for all the tickets in the world." The same is said of the target of this invention.
2.2.4 XML ticket : accepted digital ticket definition language There is an activity which formulizes the accepted digital ticket definition language with which Nippon Telegraph and Telephone (NTT) takes the lead, and is acting, and which is called an "XML ticket." This definition language and the specification of this prototype are not contradictory to this invention at all. This invention generates a digital ticket safely how, and the digital ticket of the format with this common specification is [/ what should be included] related to whether it returns.
[0051]
Ko Fujimura of NTT Information Sharing Platform Laboratories Yoshiaki Nakajima, And Jun Sekine is writing that World Wide Web offers the information distribution infrastructure for the digital contents of various classes used in everyday life. A digital cash, a micropayment (micropayment), and payment infrastructure like an encryption credit card are also established. However, winning popularity return of a duplex is prevented and neither the same digital medium as the ticket of paper which enables dealings of various rights, nor infrastructure is established yet.
[0052]
For this reason, Mr. three of Fujimura, Nakajima, and Sekine is going to develop the accepted digital ticket system which can circulate all kinds of right. A digital ticket is a digital medium which guarantees a right of a certain kind to a ticket owner, and a software license, a resource access ticket, an event ticket, an aircraft ticket, etc. are included. In order to circulate the digital ticket of various classes using a common ticket processing system, they have proposed circulating a ticket by interpreting the anonymity specified as the ticket itself, transferability, and a ticket property like an approach to return in a general-purpose digital ticket framework using the generalization ticket definition language based on XML.
[0053]
The conventional digital ticket system is developed by each application. However, Mr. three of Fujimura, Nakajima, and Sekine is sure that a generalization digital ticket system is required for the following reasons.
[0054]
(1) Supposing a ticket processing system must develop a system for each applications of each including a ticket issue system, ticket Wallet (ticket wallet), and ticket check system, the operation cost of these components will become high. For example, it is impractical to develop the system according to individual for the application for which only 20 sheets publish a ticket.
[0055]
(2) It is desirable to manage various tickets using common "ticket Wallet" who had the uniform collection view (collected view) like actual physical Wallet, and to store a cache, a credit card, an ID card, and various tickets together for a user.
[0056]
(3) New network business like cancellation, package-izing, and insurance deposit box service is manageable if all tickets are manageable to homogeneity. Probably, it will be difficult to manage such business and to store a success, when the format for digital ticket circulation and a protocol are dependent on a ticket.
[0057]
Mr. three of Fujimura, Nakajima, and Sekine specified the following requirements to generalization digital ticket definition language as a result of the investigation to their various physical tickets.
[0058]
(1) Compound possibility. Language must correspond to the compound ticket which consists of many subtickets. Usually, since it is published when a different engine publishes a ticket or they differ, there are many cases where a subticket must be published separately from the original ticket.
[0059]
(2) Status management possibility. Language must be paid and must correspond to the definition of the property with which value changes dynamically during circulation like reservation or the

acknowledgement status, for example. In addition, enabling these change by the document with a signature describes the difficult thing.
[0060]
(3) Machine understanding possibility. Language must support the definition of the semantics of a ticket. If the service or the task which a ticket guarantees is understood by a purchaser and the vender objective before it performs a transaction, the number of dispute resulting from misunderstanding of the semantics of a ticket will decrease.
[0061]
(4) Effectiveness. Language must be able to do the efficient definition of a ticket. This is because it may be stored in other devices with which a smart card or memory was restricted. A data transfer time is also taken for a long time, therefore it may not be accepted, so that a definition is long. For example, the high engine performance is needed for winning popularity return of an event ticket or transportation pass.
[0062]
(5) Circulation controllability. Language must prepare a parameter required in order to enable flexible circulation control. As shown in Table I, the anonymity of a ticket, transferability, and the approach of returning must be specified in a ticket definition. In addition, dealing also with the requirements which progressed further is desirable. For example, a ticket can be circulated between the members of the group who registered, or it enables it to publish a ticket only at the store judged to be proper.
[0063]
(6) Security. The previous researcher has noticed that language must prepare a parameter required in order to obtain security. (This invention teaches that an approach and the contents (it is not the language showing the contents) of a ticket are what gives security.) A digital ticket system must correspond to the facility (facility) which prevents duplex receptacle return like a digital cash system. An online currency check system or an alteration-proof device like a smart card, and a digital signature technique are needed for this.
[0064]
The researcher adopted the extended markup language, i.e., XML, as a base language of generalization digital ticket definition language. It is because they claim satisfying them as the above-mentioned requirements are described below.
[0065]
(1) Compound possibility. It is required that a compound ticket can be defined using an XML link. It is required that the compound ticket with which a subticket circulates on the Internet can be carried out easily. Especially this facility is useful when the check in online is required as opposed to the ticket canceled in many cases.
[0066]
(2) Status management possibility. It is required that the state-transition property of a ticket should be defined as homogeneity by attaching a value fluctuation ticket to a constraint assignment imperfect link.
[0067]
(3) Machine understanding possibility. The semantics of a ticket is defined using a resource description framework (RDF) model, syntax assignment (see the <http://www.w3.org/TR/REC-rdf-syntax>), and a resource description framework (RDF) framework (see <http://www.w3.org/TR/REC-rdf-schema>). The laminating of these is carried out on XML. This is demanded as simplifying retrieval of the ticket on the Internet far.
[0068]
(4) Effectiveness. Instead of defining the contents of the ticket itself, it is required by circulating a link to contents like the image of a ticket, or the detail of a contract that the size of a ticket should be reducible. The link is assumed to offer the newest information naturally on the Internet. For example, an event ticket is good to include the link to the location where an event is held, after an event is postponed by the reason of a rainfall or others.
[0069]
(5) Circulation controllability and security. XML is the comprehensive language designed in order to

describe all structured data, therefore can define all parameters required in order to control circulation of a ticket. Establishing a control parameter required in order to satisfy these requirements, or a security parameter does not have great effect on language as a ticket processing system.
[0070]
R. D. Brown, "Digital Signatures-for-XML", IETF-Internet-Draft, January 1999; K. Fujimura and Y. Nakajima,"General-purpose-Digital-Ticket-Framework", 3rd USENIX Workshop-on-Electronic-Commerce, Refer to reference for August 1998, pp.177-186 (<http://www.usenix.org/publications/library/proceedings/ec98/fujimura.html.>. Moreover, K.Fujimura of a publication schedule, Hiroshi Kuno, Masayuki Terada, Kazuo Matsuyama, Yasunao Mizuno and J.Sekine, "Digital Ticket Controlled Digital Ticket Circulation", and Y.Nakajima and K.Fujimura, Also refer to non-published manuscript "The XML Ticket Specification". Moreover, refer to XML Schema Requirements, The World Wide Web Consortium, Note, and February 1999 (see <http://www.w3.org/TR/NOTE-xml-schema-req>).
[0071]
As relevance over this invention of these researches, all are applied. About the mode which it generates safely, it is circulated and returns a digital ticket, there is no objection in expressing the information in a ticket (information on others like the geographical site which can further purchase the pattern of ticket circulation, and a ticket) in advanced language like XML, and this invention also actually has the point on which it agrees in it.
[0072]
2.3 Digital signature This invention noted adopting the concept of the practice in a digital signature and encoding technology. This invention operates completely with the method with which many which generate a digital signature differ.
[0073]
For example, one side has a public key (N, e) and a private key (N, d), N is k-bit modulus and the product of the two bit (k/2) prime factors and e, and d**Zphi(N) * fill ed**1modphi (N) with a Rivest Shamir Aldeman public key cryptosystem (RSA). RSA function f:ZN*->ZN* is defined by f(x) =xemodN, and the reverse x-1:ZN*->ZN* is defined by f-1(y) =ydmodN (x y**ZN*). Here, ZN* shows relatively the numerical set between 1 which is base thru/or N-1 to N. Function f can be used for encryption and can use a function f-1 for decode. f is an one direction dropping door (trapdoor one-way), roughly, if the assumption generally performed does not know d (or prime factor of N), I hear that it is difficult to calculate x=f1 (y) from ZN* to y pulled out at random, and it has it.
[0074]
In the paradigm widely used in order to sign Document M, "hash" y=Hash (M) which exists first is calculated and, subsequently to x=f-1(y) =ydmodN, a signature is set. In order to verify that x is the signature of M, f(x) =xemodN is calculated and this confirms that it is equal to Hash (M). This technique serves as a foundation of some existing criteria.
[0075]
(Outline of invention)
Especially this invention is ordered from (1) insurance on a communication network like the Internet containing World Wide Web through a communication channel about a digital instrument (although externally called the "digital ticket", some of the concept is large), and relates to the digital instrument which can be distributed to (2) insurance. Once it distributes to a purchaser, a digital ticket is the plaintext and attachment image (and still more nearly another thing.) which displayed on the computer screen (iii) after that, or were printed preferably. It investigates with the gestalt discussed below, and all the persons that possessed the digital ticket a purchaser or after that read the purpose of a digital ticket clearly, check it by looking, and agree on it, and what is kept in mind correctly is made possible. By a digital ticket carrying out [(iv)], by the purchaser, although a compact physical gestalt, the piece of paper most generally printed, or frequency is low, it returns to the memory device in which transportation like a smart card or a computer disk is possible. a certain rating determined when a digital ticket was stored in (v) insurance, and was conveyed to the location (determined when a ticket is

distributed first) which it is at a certain time with this physical gestalt and a ticket was purchased -- most generally it returns for entrance in an event. the time of being repaid for winning popularity return -- a digital ticket -- (vi) -- or [whether it is quick, and effectiveness is judged and verified, without spending insurance and costs, and a ticket is just, and an alteration] -- ******** -- a clear judgment is made. Moreover, it can also judge [whether it is repaid for the event with them, and]. [there are more same tickets or its copies than 1 time, and same]

[0076]

1. Quality of digital ticket by this invention The digital ticket of this invention has high cost-performance nature. That is, order, creation, processing, transportation, and liquidation are easy for this, it is efficient, and does not require costs.

[0077]

Especially a part such of a digital ticket is generated in a ticket purchaser's network connection computer, and is not intensive on count. Such count is small Java (trademark) which runs in the browser of a consumer's computer usually. It is efficiently realizable with applet. (Although a ticket purchaser's network connection computer is usually still more powerful, it does not necessarily meet.) The purchase of a digital ticket and transmission are not accompanied by the network communication of a lot of information at all. Therefore, the purchase of a digital ticket is usually as quick as processing of electronic commerce, or ends more quickly than this.

[0078]

The purchase of a digital ticket is as easy as processing of all electronic commerce. A purchaser does not need to be made to consider a password, a code, and no keys about the order concerned, and does not need to keep it in mind.

[0079]

That is, cheaply and finally the physical media of a digital ticket can be thrown away. The physical media of a digital ticket is a 2-D bar code in usually, and, usually, is most printed by the paper of the shape of a rectangle of the size of a number square inch evenest usually.

[0080]

Usually, the digital ticket of this invention is purchased very quickly, is created, as special thing, returns and can be carried out. A ticket is the same time lag as any purchase, and is usually generated on the Internet. Usually in spite of the elaborateness and the amount (extent) of the information included in a digital ticket, it prints easily as a 2-D bar code which a text and graphics accompanied with the graphics printer of one which is driven with a user's browser and operating system software of general formats. A duration is only dozens of seconds.

[0081]

As most important thing, it is raised that winning popularity return of a ticket is the wand usually connected to the pocket computer (always connecting with a network is even unnecessary) of a ticket ticket collector and a porter, and must scan a 2-D bar code. Reading of a ticket is performed at a high speed, is essentially errorless at a foolproof (foolproof), and is unrelated to a ticket ticket collector's intelligence, industry, or its lack. A ticket ticket collector's computer makes all judgments. It sets in a situation unusual usual regardless of how a ticket ticket collector's computer functions on a very surprising thing, and various information in a digital ticket is decoded. Only by whether for the indexation guide to the 2-D bar code of the sold effective ticket to have been printed when and where, and to have been distributed by the porter before the event It is possible to actually check the effectiveness of a digital ticket manually, without using a computer.

[0082]

The digital ticket of this invention is safe in many respects.

The digital ticket is safe in manufacture. The part protected in the code of a just ticket can be created only by the ticket manufacturer and the vender in a safe facility. Furthermore, the security of the digital ticket in the hand of the purchaser of a ticket is dependent on neither of the physical devices, and dependent on a code. It is difficult even for impossible level to create an effective digital ticket deceitfully in fact. Although the information transmitted in each of the two directions of [between a

ticket consumer / purchaser, and a ticket provider / vender] is enciphered, the security of a digital ticket is based [not only based on crypt analysis-security but] also on the physical security of a key called a signature key, and this is known by only the ticket manufacturer / vender.
[0083]
The digital ticket is safe in winning popularity return. Although the unjust duplicate of a just digital ticket may also be possible, even the digital ticket first shown only once [simple] depending on the case can return about the gap, one holding, or the event reserved by actuation of a ticket. It is essentially worthless to make the copy of an effective digital ticket.
[0084]
The security of a digital ticket can be seen. It includes detecting an inaccurate 2-D bar code most preferably by detecting an alteration or an inaccurate digital ticket easily on the inaccurate ticket repaid on the display which a computer drives by being near the just 2-D bar code which the specific ticket should own if just, and displaying. Such a vision display gives a vision display exact about it being considered by those [both] that are going to repay a porter and a ticket that a ticket is [why] inaccurate.
[0085]
Purchase and winning popularity return of this invention are the direct transaction of ticket receptacle return people and ticket ticket collection human being (by winning popularity, there may be no either or both sides of return people and ticket collection people, also when it is the same people as a ticket purchaser / consumer, or a ticket manufacturer / vender) between a ticket purchaser / consumer, and a ticket manufacturer / vender, and the break in of a third person is completely unnecessary. [a digital ticket] directions especially with easiest purchaser/consumer of a digital ticket, i.e., (1) ticket, -- purchasing -- (2) -- what is necessary is just to print it, to understand returning the ticket which carried out (3) printings, and to follow it
[0086]
Purchase and winning popularity return are anonymously possible for the digital ticket of this invention. According to this description, transferring to people from people is also possible. Although a ticket can be manufactured anonymously and it can show The original possessor of a ticket or a former possessor asserts the theft of a ticket. When this occurrence is notified to the police, more generally from all a victim's (it claimed) (of course, the rare copy of the actual ticket made by the victim is included) records From the record (responding to all the secret nature of an event of a vender's volition) which has alternatively the ticket vender who can hold, it is at the presentation time, the ticket stolen (as claimed) can be recognized, and a presentation person can be specified as the police. Even if anything does not have a meaning thing in a ticket like the specific seat number clearly as for this, it is effective.
[0087]
When the original purchaser of a ticket wants the identifier of his or her, the address, an identification number, etc. to be shown on a ticket on a safe cipher, a plaintext, or both sides although purchase and/or winning popularity return can be performed anonymously if the digital ticket of this invention is required, or if desirable, this is made easily, and according to a possibility that to be possible will be considered by the purchaser, custom-made ** of it was carried out, and it creates the digital ticket which loaded data. Actually including data in this way recommends the honest customer "who does not want to separate from the body the ticket purchased justly."
[0088]
Winning popularity return of the ticket after resulting in an effective understanding of the effectiveness of the marketing strategy which divides, it not only adds such population statistical information, but divides the time amount and the amount of dollars of ticket sale, and determines a ticket price according to the time of ticket purchase which originates when a ticket vender most generally sells a digital ticket first on the Internet, although anonymity is completely satisfactory for each ticket holder and user, and correlation attachment ****** are also make. Since the move and the re-move are usually easily [at the appropriate time] possible for the digital ticket of this invention at holders, all the rights in the ticket set as the object of division can be divided. For example, when only 5 times is effective, five different

persons can use a ticket for the film in the morning when a ticket does not specify the date only once respectively at the time of day same during the morning, or different time of day. (Winning popularity return of a ticket to many events is performed by the network-like computer which memorized partial receptacle return of an intact a large number use ticket and a ticket.)
(Under this invention, it is also instead possible to supervise and control all fields by real-time absolutely [ticket issue and a ticket receptacle return process] using a computer contrary to the concept that the anonymity of a ticket purchaser / ticket receptacle return people can be saved.) Therefore, the time amount of a game is telephoned in a football stadium, and those who accessed the data which remain on the computer of "Doctor Jones" can also tell what "Dr.Jones goes into the gate E3 at 2:22PM, and the appointed seat is 43L22".
The price total amount can be repaid without re-owning a digital ticket physically cancellable [the digital ticket of this invention] therefore.
[0089]
The digital ticket of this invention is supple and various. Even if it can set any one ticket by the combination of rating of all requests and shows which one event a ticket (or showing there is also nothing), it is uninfluential in case it is behind shown for another event. Much copies may be printed when [in which the paper which printed the purchased ticket was thin and was worn out for use] it is expected that it case or wears out (however, don't return to coincidence deceitfully.). Refer to above.
[0090]
A single use ticket serves as wastepaper of a ticket potentially, without damaging physically in an event, without not being collected but usually spoiling value. While judging the effectiveness of a digital ticket by a reader's actually letting the printed digital ticket pass, and reading the 2-D bar code by the side of the observation The information which printed advertisement or a coupon, and obtained ** after the event to the observation side at the induction-time for the ticket holder, For example, "Save $4 With This Coupon -- The information [like] Dine on Pizza at Joe's Pizza Parlor" is distributed. The digital ticket is ecologically healthy. Clearly, this does not contain plastics, the expensive hologram, and the thing of such a property at all.
[0091]
The digital ticket of this invention gives the correctness proof of itself, and if it is required, it is enough to also present a court. When a certain man presents a fake ticket (in or the case stolen goods), this can be judged immediately. Even if a porter's computer uses the secret cryptographic key, it is not necessary to solve this key (for it to be able to set to the legal indication accompanying a criminal action like), and to prove that the repaid ticket is a fabrication article.
[0092]
On the contrary, when a ticket manufacturer / vender neglects fulfillment of delivery to the just purchaser of a ticket of a product [finishing / an agreement], this ticket manufacturer / vender can find immediately having created the restricted contract completed on all the conditions related when [most] contained in the data of a digital ticket. A ticket with just ticket manufacturer / vender is a copy, when it is claimed with a false that it has returned before, this randomness can also be tackled, but when winning popularity return of a ticket is interactive, it restricts.
[0093]
the digital ticket by this invention may be considered in this way -- all advantages are almost connoted. The conditions recognized in relation to the digital ticket by this invention it may judge that is not the optimal are very few, and do not almost have importance.
[0094]
To the 1st, one of those who executes by proxy instead of a ticket consumer or a consumer like a commercial ticket seller purchases a digital ticket ordinarily by the Internet. The connection with a communication network, especially the connection with the Internet serve as the only practical method which obtains a ticket as a matter of fact.
[0095]
By the surrogate of the purchaser of a ticket, his, or her, a ticket must be printed, must be stored on a

portability memory medium, or must be stored [2nd] on a smart card. Respectively, the ticket purchaser has to own the smart card writer for the computer printer, the disk drive, etc.
[0096]
With it being unrelated to there being a lot of [rating which a ticket gives / 3rd] monetary value, since a purchaser prints a digital ticket, he does not pass in a simple appearance but it is thought that a color is also black and white. This only means that a digital ticket may not look expensive like the right which it materializes.
[0097]
the quality and the throughput of whenever [highest / in / to the 4th / ticket verification, ticket receptacle return, and the monitor in the gate] -- the (i) computer -- desirable -- a network computer and (ii) digital ticket reader -- most generally an optical reader is needed. Near the event related to a ticket a location or near it, power is usually needed. Although it does not become ticket verification and the dependability element (serial reliability element) in which it receives and which a single computer and a reader follow in a return process, the requirements for fail-safe may arise for the large spectators who are waiting for the quick entrance processing to the event by which terrible **** was carried out. The (i) computer and (ii) reader hardware to be used are usually reliable, and/or are redundant and prevent that processing of a digital ticket stagnates or is overdue. (Probably the repaid ticket should be compared with the ledger of the ticket currently printed beforehand sorted with entrance opening of an event, or it should describe that it is also possible to enter those who only show a ticket, when having not gained the pocket printer and an electronic entrance system break down in addition, although most anticipation visitors to an event have a just ticket.)
the 5th -- and finally, by the excuse that the ticket manufacturer / vender is receiving reservation of his event superfluously, and a ticket is copied, by the rare case where it is said that entrance of the just (digital) ticket holder who arrived later is refused, if winning popularity return of a ticket is performed interactively, it can be come so much out of this fraud action (digital), and it can be proved from the ticket itself. For that, it is required for the digital ticket to usually be materialized by the smart card. (In addition under this ticket issue and a ticket receptacle return procedure, it comments almost on the ability not to prove definitely about superfluous reservation of the event of a nonreserved seat.)
2. the digital ticket distribution approach therefore, the voice of this invention -- one [like] -- a "ticket" supplier company -- digital one -- this invention is materialized in the approach of having computerized which can distribute a "ticket" to a "ticket" consumer through a communication channel.
[0098]
A ticket supplier company's computer transmits the data about the incident (occurrence), i.e., an "event", which may have the authorization cut-form called a "ticket" through the communication channel first to an anticipation ticket consumer's computer. (i) Generally an incident is an event, generally the (ii) communication channel is World Wide Web, and, generally an authorization (iii) cut-form is an entrance ticket. However, the approach of this invention is not necessarily restrained by the application in such (i) use, the such (ii) communication channel, such (iii) time amount, space, or a property. For example, it purchases at a store, and carries into works, and digital "ticket" can also be returned for a certain goods.
[0099]
However, an anticipation ticket consumer acquires a ticket for the event which specification chose, decides to become a ticket consumer, and makes the computer of his/her usually generate a number R. This several R contains (i) random-number component at least. Three steps which pioneer are removed and it is also considered that "the 3rd antecedent" finally serves as a digital ticket.
[0100]
Several R can also be accompanied by including other information, such as criteria over a ticket to pay, or these, when the (ii) consumer's identity, the event which asked for the ticket (iii) and the number of visitors, and/or (iv) payment are required additionally as an option. being careful -- it is necessary to include neither of these information (ii)-(iv) in several R, and several R should contain only (i) random-number component. It is desirable that that it is completely an option can also admit presentation of information of his/hers like subscription of the identifier of the consumer to several R inside (and inside

of the digital ticket with which a consumer is provided ultimately), and when not agreeing that a consumer offers this information, there is no failure in a digital ticket issue process succeedingly, and it is substantially of the same quality.

[0101]

Next, a ticket consumer's computer calculates several R one-way function (R) (R), i.e., hash, i.e., h. Any of the function with which many which are hard to count backward on count so that several R can be derived from the original hash (R), and are accepted mathematically differ are sufficient as this one-way function. SHA1 and especially an MD5 function are suitable, and desirable. It can be considered that hash (R) is the antecedent which carried out 2 step removal, i.e., the "2nd antecedent", and, finally it serves as a digital ticket.

[0102]

Next, this calculated hash (R) is again transmitted to a ticket supplier company's computer through a communication channel from a ticket consumer's computer. Additional ticket ordering data like either of information (ii)-(iv) can follow on the 2nd transmission of hash (R), and, generally then, is. All the 2nd transmission can also usually be sent on a safe channel (SSL, i.e., secure socket level) which is established between a ticket vender's computer, and the server on the Internet and the client computer of the ticket consumer who is running the browser program. However, it is only indispensable to transmit hash (R) by the approach of this invention. For example, it can imagine distributing the ticket for a set event to all visitors in the order of arrival freely. In this case, additional ticket ordering data is not actually required.

[0103]

A ticket supplier company's computer receives hash (R) and all supplementary ticket ordering data on a communication channel. Filling a ticket demand, a ticket supplier company's computer attaches the additional information I to hash (R). That is, it becomes like I||hash (R). The information from a ticket purchaser is offered, and this additional information I can contain that either, when it wants a ticket supplier company to include such information in a ticket. however -- it should annotate -- even if there is neither a seat nor a ticket price, in order to specify at least the specific event which sold the ticket, I hear that this information I is meaningful to a ticket supplier company, and he has it. The additional information I may actually be potential very large.

[0104]

When a ticket demand is filled, a ticket supplier company's computer creates still more nearly another digital ticket which signed with the signature key s. Only a ticket supplier company understands this as what [what carried out the digital signature to the combination of hash (R) and I] (s, I||hash (R)), i.e., Sign. It can be considered that this number Sign (s, I||hash (R)) is the antecedent which carried out 1 step removal, i.e., the "1st antecedent" which finally becomes a digital ticket. Subsequently, the 1st antecedent Sign of a digital ticket (s, I||hash (R)) is transmitted to a ticket consumer's computer from a ticket supplier company's computer through a communication channel. therefore, this number and this 1st antecedent Sign (s, I||hash (R)) -- both the (i) supplier company and a consumer -- being sudden -- getting down -- (ii) -- since the specific event which sold the ticket is specified at least (even if there are not a seat, a price, etc.), a supplier company has a meaning, and he has potential possibility (iii) of including additional big information potentially. [at least]

[0105]

Next, a consumer's computer attaches several R to this number Sign (s, I||hash (R)), and forms Sign(s, I||hash (R)) ||R by this. Finally, this serves as a digital ticket.

[0106]

This number Sign(s, I||hash (R)) ||R is usually composed as a two dimensions bar code of predetermined size, and is displayed. PDF417 and QR two dimensions bar code specification are desirable.

[0107]

A ticket consumer's computer calculates a digital ticket from both the received information (namely, Sign (s, I||hash (R))) and the stored information (namely, R), and writes it in the storage which can subsequently convey this completed digital ticket Sign(s, I||hash (R)) ||R.

[0108]
If this storage fits the interface so that the digital ticket with which a consumer's computer is stored in transportation and the interior may be searched, it is good also as memory of itself. If the consumer owns this storage, it is good also as a smart card, a magnetic disk, or memory of CD/ROM. Although a digital ticket is stored, it is more expensive than the need or a desirable thing, and these device and its medium come to hand, and ****** and its storage capacity which it has are far large current (around the 2000 time).
[0109]
As for a storage, printing by a consumer's computer is desirable as ordinary paper. The ticket of paper shows all the comprehensive information about all information, the specific event which can be offered further (iii) as an option, and a specific specific ticket to (ii) ticket supplier company and/or one consumer whom either of the ticket consumers itself can offer as an option as the (i) two dimensions bar code and an option. for example, the case where a ticket consumer presents the identifier of his/her -- the ticket of paper -- (ii) -- this identifier can be printed. usually -- coming out -- (ii) when the event which applies the (i) ticket will except trifles, for example if an identifier is on a ticket so that it may discuss below although a ticket holder's identity needs to be checked because of use of a ticket -- condemnation [with one of unjust individuals or groups], duplicate or he / she/-- when their ticket is asserted, suppose that it is useful. Furthermore, for example, the comprehensive information about an event (iii) can also include the seat where the location of an event, time, and a digital ticket are effective. being careful -- when shown as this information (ii) and (iii) an option, I hear that it must not be regarded as the deterministic information on the effectiveness of a ticket, and justification, and it is. Effectiveness and justification are judged by only the (i) two dimensions bar code. The additional information on an option (ii) and (iii) should regard it as the gestalt of useful "help", in order to carry out "it having to hand" and/or "a classification" of the fact of a certain kind potentially and/or to publish to an inquiry clerk (attendant) for both a ticket supplier company and a consumer at the time of improper use of a ticket, or deceitful winning popularity return. (When a ticket is used normally and can return without a fraud action, it is required for nobody that all related information should completely pay attention for all of this additional information that it is automatically proved and can be printed as an option on a digital ticket by computer.)
The approach of this invention progresses to use of a digital ticket by the ticket purchaser in the event which specification chose after storing by distribution to the consumer of a digital ticket, and the purchaser of a digital ticket.
[0110]
This needs to repay the digital ticket in [which can be conveyed] a storage for entrance in the event which conveying the storage which wrote in (i) digital ticket, and which can be conveyed to the event which specification chose, (ii) verification, and specification chose, and (iii) to read perfect digital ticket Sign(s, I||hash (R)) ||R in the storage which can be conveyed.
[0111]
The computer which reads a ticket (event) involves as secretly as a ticket manufacturer's computer. (As long as a communication link is suitable, and it is in the situation physically, an event computer and a ticket manufacturer's computer may be the same even anywhere.) That is, the computer (event) knows the digital verification key v of a ticket computer, and the digital verification key v is equivalent to a ticket manufacturer's digital signature key s. If digital ticket Sign(s, I||hash (R)) ||R is read, R will be extracted and it will use behind. subsequently, Sign (s, I||hash (R)) is decoded using the digital verification key v, and I||hash (R) is acquired (although this will be remembered -- completely -- a function -- not but, it is only only the combination of I and hash (R).). Next, a consumer's computer newly calculates new hash (R) using the same one-way function as having used before using extracted R. It compares with hash (R) which newly (**) calculated decoded hash (R).
[0112]
Read Sign(s, I||hash (R)) ||R is decoded by use of the digital verification key v in (1) Sign (s, I||hash (R)) part, I||hash (R) is obtained, and a digital ticket is a genuine article when hash (R) which carried out (ii)

decode is equal to newly (**) calculated hash (R). A digital ticket is fabrication when either of these two conditions is missing. That is, when (i) decode or (2) comparisons go wrong, a ticket serves as an invalid.

[0113]

When fulfilling both conditions, decode which obtains I||hash (R) using the digital verification key v is performed. When newly (**) calculated hash (R) is equal to the same amount as being stored from the first in a digital ticket at the time of the distribution for the event which that production and this specification chose, A ticket is surely a thing for a proper event (I defines), and must evaluate further whether it is that the specific ticket was shown in this way first. When a meaning is shown first the contents of the read digital (and it decoded) ticket, as for the holder of a digital ticket, entrance in an event is permitted. On the contrary, when a meaning is not shown the read digital ticket such first, the holder of a digital ticket is usually denied entrance.

3. Digital ticket distribution system In one with the another mode of this invention, this invention is materialized to the system which distributes a digital ticket through a communication network. Probably, in this mode, it will be good to examine how the functionality of this system is classified. It examines that what is correctly transmitted that what is correctly performed in each of the computer of a ticket consumer and a ticket supplier company, and on a digital communication network.

[0114]

Several R is calculated to the 1st. the computer of the ticket consumer by whom this system was connected to the communication network -- containing -- (i) -- (ii) The one-way function of R is calculated [2nd] and hash (R) is generated as ticket ordering data. To the (iii) 1st on a communication network The hash(R) ticket ordering data calculated by the 2nd to a ticket supplier company's computer as the order of a ticket to the event which specification chose -- transmitting -- (iv) -- to the 1st What carried out the digital signature to the combination of hash (R) and Information I, Attachment of R to this digital ticket antecedent Sign(s, I||hash (R)) || is calculated to the 3rd. Sign (s, I||hash (R)) -- as the digital ticket antecedent -- receiving -- (v) -- as a perfect ticket -- Sign(s, I||hash (R)) ||R -- giving -- (vi) -- it stores in the storage which can convey perfect digital ticket Sign(s, I||hash (R)) ||R calculated to this 3rd [the] to the 1st.

[0115]

A ticket supplier company's computer is also connected to the communication network. (i) To the 2nd, the hash(R) ticket ordering data transmitted the 1st is received from a ticket consumer's computer. (ii) The information I about the right of others which an event or a ticket has is added. What carried out the digital signature of hash (R) and Information I which were received to this 2nd [the] to the 4th, and was enciphered, (iii) Sign (s, I||hash (R)) is calculated as the digital ticket antecedent. Namely, as (iv) the 2nd transmission The Sign (s, I||hash (R)) digital ticket antecedent calculated to the 4th is transmitted to a ticket consumer's computer through a communication channel.

[0116]

a communication network -- (i) -- the 1st -- the 1st communication link -- carrying out -- transmission of the beginning a ticket consumer's computer -- reception of the 2nd of a ticket supplier company's computer -- corresponding -- making -- (ii) -- the 2nd communication link is performed to the 2nd, and it is made for transmission of the 4th of a ticket supplier company's computer to correspond to reception of the beginning a ticket consumer's computer

[0117]

4. Digital ticket In one [still more nearly another] of the modes of this invention, a ticket consumer materializes this invention on a communication network at the digital ticket supplied by bidirectional processing with a ticket supplier company. In this mode of this invention, it concentrates [what is in a digital ticket correctly, and] proper and correctly about which sequence of information actuation and exchange leading to these contents.

[0118]

A digital ticket is materialized in [which can be concreteness conveyed containing Sign(s, I||hash (R)) ||R] a data carrier. (i) R It is a ticket consumer's secret random number, and (ii) hash (R) is a number

which is a one-way function of R. I(iii) ||hash (R) It is, attachment, i.e., combination, with hash (R) of the information I about the event (or right) which a ticket has. (iv) Sign (s, I||hash (R)) The digital signature of the combination with I||hash (R) is carried out to a ticket supplier company's secret signature key s, it enciphers, and (v) Sign(s, I||hash (R)) ||R attaches R to this digital signature code.
[0119]
Furthermore, each origin of these mathematical amounts that are in a detail in a digital ticket may be described to either (i) ticket supplier company's computer, or (ii) ticket manufacturer's computer. The digital ticket which the ticket consumer supplied by bidirectional processing with a ticket supplier company on the communication network is materialized always in [which can be concreteness conveyed containing Sign(s, I||hash (R)) ||R] a data carrier. However, the sequence how this number is settled in a digital ticket consists of some steps in detail.
[0120]
It is the number with which R has the origin in a ticket consumer's computer in the beginning.
The hash calculated [2nd] about the one-way function of R, i.e., R, or hash (R) has the origin in a ticket consumer's computer.
[0121]
This number hash (R) is attached to the event (or other tickets) information I in a ticket supplier company's computer the 3rd.
To the 4th, this computer of a ticket supplier company also calculates a digital code with a signature based on an attached number of digital signature keys s and Sign (s, I||hash (R)).
[0122]
To the 5th, a ticket consumer's computer attaches several R to the digital code Sign (s, I||hash (R)) with [this] a signature, and generates Sign(s, I||hash (R)) ||R.
Several R has the origin in a ticket consumer's computer, is a ticket consumer's secret, and is not public.
[0123]
The digital signature key s of a ticket supplier company's computer is a ticket supplier company's secret, and is not public.
[0124]
5. Epitome which this invention simplified -- Part I This invention is not unfairly complicated. The old 2nd thru/or especially chapter 4 are not necessarily long. Although the step based on the mathematics of the approach of this invention promises to improve from this, it was made to finish it as Chapter 2 quickly. However, although there is mind that a reader will agree with this invention being accompanied by the step based on the exact mathematics which exists clearly by the point in time of this explanation "the tree being looked for and it wavering in woods," in fact, -- ******** -- it cannot be holding correctly why the approach, system, and ticket of this invention offer [how] many advantages which are safe or all enumerated in Chapter 1 "synthetically"
[0125]
Things are examined from this viewpoint. A ticket consumer's computer is generating some of random numbers (essentially) known only in itself at first, the one-way function, or the hash. This cannot generate a ticket supplier company's computer at least at first at the time before winning popularity return of a ticket. Although a ticket supplier company's computer can generate this one-way hash function only when it has a random number, it does not have this number in an initial state.
[0126]
Through a network, from the computer of the consumer who is a generator, a ticket manufacturer's computer receives an one-way hash function, and progresses to the processing which cannot generate a consumer's computer and which generate a digital signature with a signature. It does not have a consumer's computer, although this signature procedure can be performed also in itself if it has the secret signature key of a manufacturer's computer.
[0127]
Also by those who monitor a part or all of a communications traffic on the network related to a digital ticket, I hear that understanding immediately cannot judge both the random number (R in the above-

mentioned chapter) of (i) ticket consumer's computer, and the signature key (s in the above-mentioned chapter) of (ii) ticket manufacturer's computer, and there is.
[0128]
From a manufacturer's computer, a consumer's computer receives what was now signed by the one-way hash function (it transmitted before) of itself through a network, only attaches the original random number, and stores complex as a digital ticket.
[0129]
When returning a ticket first, about how the digital signature of a manufacturer's computer is decoded at least, a manufacturer's computer or the computer of a porter with more high possibility has computer and secret relation of a manufacturer, and can access a random number first immediately. This number is a clear text. Taking out this random number, a porter's computer reproduces an one-way hash function next using the knowledge of that digital verification key (v in the above-mentioned chapter) over the encryption signature of a ticket manufacturer's computer.
[0130]
When a ticket is just, it has succeeded in decode of signature data. A porter's computer has the one-way hash function of the (i) random number and the (ii) random number next. What should this carry out? Why do you only re-calculate an one-way hash function on a random number, and compare it with what already exists at hand? The digital ticket is effective when both functions are equal.
[0131]
Thus, when analysis and explanation are advanced, noticing first does not have information with other persons concerned to each person concerned among the generating process of a digital ticket. This information is hidden by the back of one direction conversion, or encryption. Consequently, to fraud by the purchaser, although it is much more important, the capacity to swindle, take or misuse the process of other persons concerned of which person concerned is restricted.
[0132]
To the seller who swindles, in an interesting thing, a purchaser has the resource of the more than which only complains, and holds future protection to it. Generally the verification key v of a ticket vender's digital signature is known publicly. Therefore, a seller is able to prove owning goods with just him/her. Although it is only the moderate importance for only participating in an event, the "dual accountability" of this invention divides and is much more important to other safe transactions like money order.
[0133]
6. Epitome which this invention simplified -- Part II This invention is larger than the detail of the embodiment.
For example, it is not necessary to necessarily regard a random number R as one random number. This may build in the information about either (i) ticket consumer, the event which is the purpose of (ii) ticket purchase or the date of other ratings, a location and/or a name, the price of a ticket (iii) and (iv) and also another data, or may combine with these. As for the indispensable concept, several R of net is random, and also when based on a ticket supplier company, it is only not guessed [include].
[0134]
Similarly, as an example, one-way hash function hash (R) does not need to be a simple mathematical Hash Function, and can also make this very thing a code as an example. It can be considered after all that a code is the gestalt of ultimate hashing.
[0135]
Next, once it turns out that it is larger than the strategy of an embodiment with the only suitable idea of this invention as mentioned above, how should he understand the claim of this specification about this invention and this invention? after understanding the above-mentioned 1st and Chapter 4, he considers the property of this invention and understands -- an option further Examine final digital ticket Sign(s, I||hash (R)) ||R, and this digital ticket is disassembled. It will be expressing with words what the digital ticket consisting of correctly by stripping the layer like an onion and going (being mathematics similarly).
[0136]

I hear that a digital ticket contains something and the random number which are a clear text, and what can be said first has it (or in a certain deformation of this invention, when enciphered, it can return to a clear text immediately by applying a presentation person's cryptographic key). The ticket consumer created something [this] and this R. However, most typically, by the time this amount R of clear texts is finally first known by the ticket supplier company, usually long time amount passes, and if it is not at the presentation time of a digital ticket, it will not be known for usual in an event to hold a ticket. A ticket consumer follows and conceals this random number from all over the world from a ticket vender by use of a one-way function hash (R).

[0137]

Next, a digital ticket also contains something. That is, it is the information I about an event to hold a ticket at least, and this information I may be guessed and is not safe. The security of a digital ticket is in the digital signature of both hash (R) and I using the secret signature key s in Sign(s, I||hash (R)) ||R. Although this amount is generally usually decipherable to anyone at a plaintext using the open key v, this cannot be performed without the knowledge of the signature key which is a private key. Therefore, only a ticket vender can make the final antecedent of the digital ticket itself.

[0138]

A porter has a secret relation with a ticket supplier company. When making digital one and a signature from public key algorithm like an RSA algorithm, even if a porter cannot sign this amount first, he can decode the amount of signatures by use of a public key. In other words, a porter does not need to perform a ticket supplier company's function and does not need to go up on the level.

[0139]

In addition, although this is desirable when a ticket manufacturer's verification key is public, anyone can reproduce the signed amount I and hash, i.e., ticket information, (R). Therefore, the effectiveness of the ticket for the resale by the original purchaser and final winning popularity return can be judged very easily. Of course, no possession of amount-of-data I in a ticket and hash (R) is performed about generation of R or Sign (s, I||hash (R)). hash (R) -- a one-way function -- it is -- (i) ticket consumer -- a source -- it is -- (ii) ticket supplier company -- a digital signature -- "-- it wraps -- having -- " -- please get down and remember having allotted throughout the inside of a digital ticket by the ticket (iii) consumer.

[0140]

Moreover, a porter's computer reverses hash (R) and it comments on it that it is not necessary to ask for the seed, i.e., R,, either. At the time of digital liquidation, this seed, this R [i.e.,], is actually given. Only using this seed, i.e., R, a porter's computer performs a one-way function again, and newly generates hash (R). It compares with the one-way function which decoded the re-calculated one-way function in order to evaluate the effectiveness / invalid nature of (ii) digital ticket.

[0141]

Thus, the digital ticket by this invention is materialized by the digital storage which can be conveyed [material]. Both the 1st sort data, i.e., a purchaser, and the seller of a ticket understand the medium from the start, and at least, for the vender of a ticket, in order to specify the specific event to which the purchaser of a ticket and the ticket were sold, it contains meaningful data. This 1st sort data has the property of an index, and by this, relatively, from many ticket purchasers, a ticket vender does being based on an identifier etc., and he can specify the purchaser of a chisel and a ticket rather than is absolute. This 1st sort data enables usual, however a ticket vender to identify absolutely a specific event and the time of day of a ticket.

[0142]

Furthermore, an important thing is that a medium also has the 2nd sort data containing the amount by which the digital signature was carried out. This is generated by computer in the following sequence from the first. (i) It generates as an irreversible function of the random number called "the irreversible function made by the 1st time" to the 1st by the purchaser of a ticket at the 1st time, and next, it generates as a digital signature of the irreversible function made by the seller of a ticket the 1st in (ii)2 time, and, subsequently (iii) to the 3rd time, generates in the 3rd by the purchaser of a ticket who

completely attaches the same random number. Here, what is contained in continuation (step i)-(iii) is indispensable at the digital ticket of this invention.
[0143]
Thus, when it is going to perform winning popularity return of a ticket, the constituted digital ticket steps on a phase and judges the effectiveness. First, a random number is taken out. Next, the irreversible function which is signed and which was made by the 1st time is decoded, and the irreversible function made by the 1st time is reproduced. Next, the irreversible function of this taken-out same random number is made again. This newly made irreversible function is called "the irreversible function made by the 2nd time."
[0144]
(i) The irreversible function made by the 2nd time is equal to the irreversible function made by the 1st time, and the ticket is effective when it succeeds in verification and decode of (ii "the data which signed"). When the irreversible function made by the 2nd time is not equal to the irreversible function made by the 1st time, or when the digital signature of a ticket cannot be verified, a ticket serves as an invalid about a specific event at least.
[0145]
The mode and attribute of these of this invention and others will become increasingly clear by referring to the following drawings and attached specifications.
(Explanation of a suitable operation gestalt)
The following operation gestalten and vocabulary with this invention fundamental in Chapter 1 are explained. In Chapter 2, it writes in a detail clearly about the design of a digital ticket issue method based on the Internet of this invention. In Chapter 3, the ticket issue method with which some are related is discussed, and it compares with the technical advantage of the approach of this invention. In Chapter 4, about the amelioration to the digital ticket of this invention, and a digital ticket issue method, some will be pointed out and it will round off at the last.
[0146]
1. Fundamental operation gestalt, vocabulary There are two main operation gestalten in this invention. (1) Since it fixes to a material medium (that is, it prints on paper), it is the electronic operation gestalt (show in drawing 2 and drawing 3) fixed to the material medium called equivalent by the writer of these formats of the printing implementation gestalt ticket 1 (show in drawing 1) which needs only the printer which is large available computer-related peripherals and (ii) flexibility disk ticket 2, the CD/ROM ticket 3, DVD, a smart card (not shown), or digital money.
[0147]
In addition, on these specifications, although the 1st person concerned to a digital ticket is variously called in the combination of a manufacturer, a supplier company, a vender, a promoter, servers, or these vocabulary, the matter under statement is guaranteed. For example, this person concerned is called "the promoter (server)" on the right-hand side of the table of drawing 5 . The same person concerned as this or other persons concerned concerning this person concerned may be called a ticket ticket collector or a porter.
[0148]
On the other hand, 2nd another person concerned to a digital ticket is variously called in the combination of a purchaser, a consumer, a customer, a browser, purchasers, or these vocabulary. For example, this person concerned is called "the purchaser (browser)" on the left-hand side of the table of drawing 5 . The same person concerned as this or other persons concerned holding the digital ticket from this person concerned may call it ticket receptacle return people or those who repays a ticket.
[0149]
Although the 1st person concerned may also be called the "generating person" of a digital ticket by the strange thing and the practice, a digital ticket is printed or the 2nd person concerned changes it into a material medium by printing or storing.
[0150]
In this specification, it will be simple to process all different vocabulary that calls each person concerned

with a word processor, and to apply one, or at most two different vocabulary or description for every person concerned. However, when done so, it turned out that an understanding of the context in which a certain person concerned is working, and this invention of both delicacy is checked. Therefore, the identifier instead of many is saved.
[0151]
2. Digital ticket using paper This invention affected the remarkable existing Internet technique, and obtained the solution with easy use.
[0152]
A consumer accesses a browser with a SSL function, trusts it and establishes [1st] encryption and authentication connection to a merchant / ticket issue server. In addition, with the operation gestalt by suitable printing of the 1st of the digital ticket 1 shown in drawing 1 , the consumer user assumes that a printer can be accessed. (Similarly, with the operation gestalt of the 2nd flexible disk of the digital ticket 2 shown in drawing 2 , the consumer user has to have the magnetic flexibility disk drive, and the consumer user has to have the CD-ROM drive which can be written in by the operation gestalt of the 3rd CD-ROM of the digital ticket 3 shown in drawing 3 .)
Using the browser of his/her, a consumer connects with the web server of ticket issue service, and purchases a ticket using a standard payment device like the transaction of a credit card. Most preferably, a ticket issue server is composed in the gestalt (and a certain attachment text as an option) of a 2-D bar code, and distributes a ticket to a consumer's browser. Subsequently, in the printing version of the digital ticket 1 shown in drawing 1 , it prints as a bar code 11. A consumer does not need to arrive a ticket at the event hall a little early to reception. The digital ticket 1 of the shape of a printed bar code is only shown to a ticket ticket collector, and a ticket ticket collector actually verifies this by the laser scanner.
[0153]
The digital data (or equivalent DS in the operation gestalt of the flexible disk of the digital ticket 2 or the CD-ROM operation gestalt of the digital ticket 3) encoded by the 2-D bar code 11 is the core of a ticket issue device. In digital postal-charge sealing, i.e., generation of "e-stamp", a server generates an encryption digital signature by this invention similarly. This is some ticket data. However, even when, as for the method of this invention, a ticket issue server receives harm unlike postal-charge sealing, an aggressor cannot take a consumer's ticket but has prepared the additional guarantee that a just consumer can be paid to the framework of return [winning popularity] of a duplex. The ticket guarantee protocol is as follows as an outline is shown in drawing 5 on the whole.
[0154]
(1) A ticket issue server and a consumer agree about the ticket information I. This information specifies time amount, a location, etc. of a venue, and, usually, contains the consecutive numbers of a ticket.
[0155]
(2) A customer's browser generates a random number R and sends hash (R) to a server through a communication network 5 (typically shown in drawing 5) (plug-in used with the downloaded Java (trademark) program or browser). ((Just to let a communication network 5 be the Internet.) What is necessary is) It is here, hash (-) is an irreversible function, and if the powerful computer which carries out long duration actuation is used, it will be thought calculative that the decision of (-) from hash (-) is possible. However, the decision of (-) from hash (-) is unrealizable by being clearly impractical on count. Since all the attempts that that this means meets and are made like exceed sharply usually both time amount left behind by rating which the cost of a ticket and a ticket guarantee numbers of times, this alternative is not realistic.
[0156]
in addition -- and hash (-) is a Hash Function which is equal to a collision further -- desirable -- several -- hash (R1) of R1 -- R1 -- several -- even if it is approaching very much from R2 and is separated only from 1 -- several -- it means not approaching hash (R2) of R2. The mathematical function SHA1 and especially MD5 are suitable, and desirable. Although the effectiveness of this desirable collision resistance and this effectiveness are related with the fallacy claim of the duplex receptacle return by the ticket vender, they are discussed below. However, for now, the security of a digital ticket is rash in it

being in the difficulty on count of counting a hash (R) function backward, and must not guess. This Hash Function actually acts only in order to protect it from all unjust actuation by the vender of the digital ticket considered to be honest, however it may see the noble-mindedness of a final digital ticket.
[0157]
(3) A ticket server / vender attaches the information (i) Existing, signs hash (R) which received, and the attached information I using (ii) digital signature key s, sets to Sign (s, I||hash (R)), and returns a consumer this (iii) amount of data that signed through the same digital communication network 5. (Here, it is assumed that x is reproducible from Signature Sign (x) with those who have the knowledge of the suitable decode algorithm from a ticket server / vender, and/or a key.) The verification key v and the algorithm corresponding to the signature key s are also sometimes usually public. However, a ticket consumer / user does not have a means to generate the amount Sign (s, I||hash (R)) signed in digital one by many [other than a ticket vender], either.
(4) A consumer/user can add or attach something to the amount of encryption, carrying out a deer, and this consumer/user attach the same R which was the base of hash (R). (Please remember that it cannot be returned, even if a ticket server / vender is never notified of this R but you want to do so.) Amount Sign (s, I||hash (R)) ||R becomes a logical digital ticket.
[0158]
Preferably, the browser of a consumer/user encodes this value as a 2-D bar code, and, subsequently prints it in the usual paper for printers. This is a physical ticket and a consumer/user has to bring this to the gate.
[0159]
Not only hash (-) is irreversible, but the requirements that it is strong to a collision suggest a delicate property. A ticket server suggests what (therefore, a user cannot be entrapped) a false cannot return an effective ticket for are irreversible. The only approach the resistance to a collision can perform winning popularity return of a duplex gives the guarantee of addition that it is the case where a user leaks the reserve (or by chance [Intentionally]) image value R.
[0160]
It consists of confirming that winning popularity return of a ticket is the reserve image of a hash value with which the R value which checked and encoded that it was a thing to the specific event which the 2-D bar code was scanned, the signature was only verified, and Information I repaid the ticket actually signed. In addition, a value R is recorded as a proof of the ticket was able to cancel or return.
[0161]
The digital ticket 1 using the paper as an example is shown in drawing 1 . The plaintext information 12 and an image 13 are specific for rating which is usually called entrance in the event which is the object of a ticket. However, this always comes out so, a certain need is not, and a digital ticket can be made without the clear reference which shows that they are the things for "secret pass." In order to prevent theft, the just holder of the just ticket of a football game may actually choose that a text or an image do not appear at all on a digital ticket. Even if it is missing, it is completely uninfluential to winning popularity return of a ticket.
[0162]
Furthermore, the digital ticket 1 using paper also shows the field 14 including the information on a ticket. A plaintext is sufficient also as this information 14, and it is read and recognized by the optical character reader (OCR). Preferably, it is in a bar code, or this information is repeated and is a two dimensions bar code 11 like [it is still more desirable and] illustration. According to PDF417 or QR specification, the printed two dimensions bar code is further much more desirable.
[0163]
For the requirements that the digital ticket 1 is conveyed to the gate in the paper, I hear that constraint of this method must be received and must constitute a return protocol from a single message, and there is. Since all verification information (it is (like R of this invention)) is solved at a single step, what prevents that those who scan a ticket claim the fallacy that the ticket was able to return before does not have anything. (The opinion of such a fallacy does not necessarily show the malfeasance by any of a ticket

vender or ticket receptacle return people.) An employee's porter may enter his friend unjustly and may send back the just holder of the stolen seat. However, if a ticket is stored in a smart card, implementation of a bidirectional processing protocol is possible. There is the following advantage in use of bidirectional processing. Those who scan a ticket can prevent performing the fallacy claim of such early ticket receptacle return. It investigates next about this.
[0164]
2.1 Disk and digital ticket using smart card The same information as being held at the operation gestalt by printing of the digital ticket 1 of this invention shown in drawing 1 and the information beyond it can hold easily in an operation gestalt like the flexible disk 2 shown in drawing 2 . It will be understood that other MAG which can convey a class and optical storing media, size and the volume, and area of this flexible disk 2 of a large number containing CD-ROM, DVD, and a smart card (not shown) correspond mostly. But the physical gestalt of these common knowledge is not separately illustrated like the flexible disk 2 of drawing 2 . It is because such no drawings are completely added to an understanding of this invention. The most interesting gestalt is a smart card (not shown) from a functional viewpoint.
[0165]
By using a smart card as a digital ticket container, as it is the following, those who scan a ticket fabricate (framing) and prevention is attained.
[0166]
A browser generates the random value R0, R1, ..., the vector of Rn-1, and is required as sending Hashes h (R0) and h (R1), ..., h (Rn-1) to a ticket server. A ticket server generates Signature Sign (s and I||h(R0) ||h(R1) || .... ||h (Rr-1)).
[0167]
A ticket receptacle return protocol acts as follows.
(1) Those who scan a ticket generate random subset C**Zn so that it may be set to |C|=n/2.
[0168]
(2) Those who scan generate Signature (C) s using a specific signature key to those who scan, and entrust challenge selection (challenge selection) by sending this to a smart card.
[0169]
(3) A smart card verifies Signature Sign (C) and verifies that C contains the element of n/2 of meaning correctly. Subsequently, it is **i ** C to those who scan a ticket. : Ri is clarified.
[0170]
In this protocol, it becomes proof without the room of the counterevidence of duplex receptacle return to have the record which contains many rather than the one half of a reserve image, since only one half of a random reserve image is clarified.
[0171]
Unlike Chaum's cut-and-choose protocol to cybermoney, this invention does not need encoding of identity information. A consumer reports physically and has to return a ticket. David Chaum and Amos Fiat, And Moni Naor; Untraceable electronic cash; in Advances in Cryptology -- Crypto'888 and pages 200-212; Refer to Springer-Verlag and 1990. (This design decision must be again taken up, when the digital ticket of this invention is used for the event or rating which does not need physical presentation.) Those (or ticket publisher) who a Hash Function is one strong (and strong in the 2nd reserve image) against a collision, and scan a ticket cannot entrap a customer because of duplex receptacle return. Commission of the challenge set C of a person to scan is continued from the place which it left, when it makes it shown in a smart card that it was in the ticket receptacle return protocol and a protocol is interrupted in what kind of reason.
[0172]
2. Related system There is related use like generating of some systems relevant to Internet auxiliary ticket issue and a coupon. About these systems, it discusses in this chapter 2 and compares with the method of this invention.
2.1 Share authorization code There are some methods of offering service similar to ticket issue. Although one of the easiest approaches is already adopted for the transaction of a telephone on the

Internet, it is using a secret authorization code as a "reservation number." Such confidential codes are memorized or it writes down, and usually, it offers only in order to identify a reservation entry uniquely in a commercial database. If a customer arrives, an original credit card and original Photograph ID will be required, and he will check in at a hotel, or a physical ticket will be received. Of course, when a consumer acts as key Inn of the code and operates the automatic gate, use of these codes can also be imagined.

[0173]

Although such a code can be distributed in a network, using is difficult for it. With the ticket to the venue in which large spectators are, if a code is not long, it will become so extensive that no fraction of effective codes is accepted. And if a code is long, a user will memorize it or will sense difficulty for acting as key Inn proper.

[0174]

2.2 ETM ETM is in the existing ticket issue system (around the 2000 time) (<http://www.etm.com/>). ETM is based on a kiosk. Usually, a consumer goes to the kiosk in the location which it visits frequently [the inside of a grocery store, or others] by usually, and purchases a ticket by using a credit card. A ticket is printed by special paper. Access to a ticket is controlled and it is assumed that paper cannot be fabricated. The card stock of an airline ticket is controlled similarly. In addition to a direct purchase, ETM also permits the purchase on the Internet by visiting the website. By the transaction of a credit card, an authorization code is obtained, this is used by the kiosk (adding to presentation of a credit card probably), and a ticket comes to hand. This Internet "purchase" is actually one of the approaches of reserving a ticket rather than an actual ticket purchase.

[0175]

2.3 E-ticket The agent who calls E-Ticket, and the event ticket which <http://www.e-ticket.net/> can already (around the 2000 time) receive on the Internet in Japan are sold. Their ticket consists of a data image and a purchaser saves it to a flexible disk. A ticket vender prepares the exclusive booth for winning popularity return of a ticket in an event site, inspects the electronic ticket stored in the flexible disk using the small computer, exchanges the ticket and electronic ticket of paper, or enters a ticket holder in a venue only through the exclusive gate.

[0176]

Since a ticket transfer medium is a flexible disk, a reading error sometimes occurs. In order to solve these problems, E-ticket announced the proposal which permutes a ticket transfer medium by ID tag (non-contact smart card). These electronic tickets are easy to copy. As a deterrent, E-ticket requires the member registration containing an identifier and a credit card number.

[0177]

2.4 E-coupon A coupon is a ticket to discount. A certain agent has already (around the 2000 time) distributed such a coupon from the website on the Internet. Internet Coupon Service and" <http://www.e-coupon.com/> --" "has distributed the coupon which set to a certain store and Liberty Production <http://www.autoshowusa.com/>, and has distributed the usable coupon to them, for example, can be used for them from their website at International Auto Show.

[0178]

According to the directions on a web page, a user displays a coupon on a screen and prints this coupon. Consequently, a user goes with the printed coupon and receives a certain discount privilege in a store or an event site. A coupon is a kind of promotion strategy, therefore is not examined [as opposed to / especially / fabrication].

[0179]

2.5 Electronic check The electronic check is the same as a ticket or a coupon at the point of encoding a single royalty. B. Clifford Neuman and Gennady Medvinsky; Requirements for network payment: The netcheque perspective; Refer to in Proceedings of IEEE COMPCON'95 and March 1995. Here, capability is a right which transfers money to receipt people's own account from the check account of a checkwriter. Since there was extensive settlement-of-accounts infrastructure in a physical check, it was proposed that it would profit by Neuman and Medvinsky in settlement of an electronic check using this

infrastructure. Such settlement-of-accounts infrastructure cannot be used for an electronic ticket, and does not have need, either.
[0180]
2.6 Ticket data Fujimura And Nakajima inspected the requirements for data encoding of an electronic ticket and a coupon. They proposed encoding data using XML and gave the list of ticket properties which should be shown. This invention and this research can cross at right angles, and two can be combined and used. Refer to the chapter of the background of invention of this specification.
[0181]
3. Compatible Hash Function It is not based on the Hash Function which performs the effectiveness of this invention, and security in the computer of selection of a random number, and the purchaser of a ticket. The main reasons performed by continuing hashing will remember that it was taking care of a purchaser to the conscienceless ticket seller who did sale of the same ticket twice (in digital one).
[0182]
However, it is possible to use a specific new method for hashing. This method is the theme of the United States patent application to PROBABILISTIC SIGNATURE SCHEME (stochastic signature method) for which it applied on February 9, 1998, and was transferred to the same grantee as this invention.
[0183]
The purpose of invention of this application is offering a new signature method the about the same as the standardized method, easy, and efficient. If it assumes that the Hash Function used as a foundation is ideal, a safe thing not only can prove the invention approach of related application, but it can prove a safe thing in strong semantics. With 1 operation gestalt using RSA, a signature is [the size of verification of a signature] the size of modulus with 1 time of RSA encryption, and a certain hashing with one RSA decode and a certain hashing. According to the statement, with this operation gestalt, the security of the method of invention of related application is closely related to the security of the RSA function itself. Moreover, instruction of this another application is extended and also offers the method of the Rabin signature which has an analog property. That is, such security can be closely connected with the difficulty of factoring (factoring).
[0184]
The specific new method for this hashing is the theme of said United States patent application for which it applied to PROBABILISTIC SIGNATURE SCHEME (probability-theory enemy signature method) on February 9, 1998 and which was transferred to THE REGENTS OF THE UNIVERSITY OF CALIFORNIA (University of California director), and is suitable for using in the system of this invention. That is, it is well-known to hash Message N on all domain ZN* of a RSA function before decode. The signature of M is fl (h (M)), and h is constituted so that the argument may be extended to homogeneity at ZN*. According to related application, such a well-known technique is strengthened by making hashing stochastic. In order to sign Message M, a signer chooses the random seed r of die length k0 first. k0<k is the parameter of a method here (please remember that it is k=|^N|). Next, a signer generates image point y=HashPSS(r, M) **ZN* from M and r using the hashing which is a specific approach. Then, a signature is x=f-1(y) =yd like usual. mod It is set to N. Verification is still more difficult. It is because it is not expectable to be unable to re-calculate the probable hash of M simply, but to acquire the same value. Verification still requires 1 time of RSA encryption, and only a certain hashing.
[0185]
The method of this another application claims that it is efficient like the well-known signature method based on RSA. Furthermore, it asserts the hashing method of related application that it is also closely related to the security of the RSA algorithm itself as mentioned above. It follows, for example, when a RSA inversion probability is 2-61 from the first (the count resource of a certain amount is used), the probability of the fabrication to a signature method becomes low almost equally (the same count resource is assumed).
[0186]
According to this another related application, the signature accompanied by "message reappearance" is

also offered. This technique decreases bandwidth required in order to send the message which signed. In this technique, Message M and its signature x are not transmitted, but die length transmits the improved single signature tau of under |M|+|x|. The verification section reproduces tau to M and checks credibility to coincidence. In the case of the security parameter k= 1024, it is claimed that this invention method can attest the message to n= 767 bits by transmitting only a total of k bits. When the signature method accompanied by message reappearance attained this, a message is appropriately inserted into a signature and the verification section enabled it to reproduce it. The effectiveness and security on count are the same as the method explained first.

[0187]

Thus, in one of the another mode of this of application, it is related with the approach of signing a data string. This approach progresses gradually, hashes (a) data string and a seed value, generates s hash value, and encodes the given parts of the (b) hash value, a seed value, and a data string at an image point, and applies a (c) given decode primitive to an image point, and acquires a data string's digital signature.

[0188]

the voice of this another application -- in other one [like], the data string K who has a part for a part for part I M1 and part II M2 can be signed, and a data string can be reproduced from M1 and M2 about the computer practice which attests this. This approach hashes (a) data string and the random seed r. The step which generates hash value h (r, M), and the step which encodes a part for part II M2 of (b) hash value h (r, M), the random seed r, and a data string at the image point y, (c) A decode primitive is applied to the image point y, and the step which acquires a digital string's digital signature x, and the step which relates the (d) digital signature x with a part for a data string's part I M1 are included.

[0189]

Therefore, the signature method based on RSA of this another application essentially claims that the optimal effectiveness coalesced in the attractive security property. In this method, one suitable signature routine needs one RSA decode and a certain hashing, verification needs 1 time of RSA encryption, and a certain hashing, and the size of a signature is the size of modulus preferably. When an ideal basic Hash Function is given, an only safe thing not only can prove this method, but it has the security which is closely related to the security of RSA. In one of the alternative implementation gestalten, all the above-mentioned descriptions were maintained, in addition it also has message repeatability. This technique is extensible so that the method to the signature based on Rabin or the signature using other one-way functions may be given.

[0190]

This technique is suitable for using with this invention. However, the digital ticket issue system and approach of this invention of not needing such advanced hashing and signature technique are clear. The code of this invention is very powerful and it is mainly to have described the hashing and signature technique of this another invention and application as an example that it can be completely connected with the present front line which progressed most. Although this invention can be materialized to the small printing field of cheap paper, it will be understood by the practice person of a code technique that the informational elaborate nature and the security which were shown in this way are very large. The level, the crypt analysis-security, and others of the security always stirred up in the use in the system of this invention and the real world of an approach protect worth of all the tickets it not only will probably protect appropriately worth of the single ticket of 100 U.S. dollar extent around 2000, but sold to a certain event, and if they be main sport events, it be rare that it can become the what 10 million U.S. dollar, either.

[0191]

The contents of other applications are given by Regents of the University of California such whose access is the common grantee of both this application and another application, so that it shall be contained also in this application by this reference and access to it is needed for issue of all patents over this application, or all other situations with reference.

[0192]

4. Conclusion According to this invention, the method which can purchase and distribute a ticket on the Internet was taught. An artificer will check these methods, if it is practical and moderate balance is obtained between security, consumer accessibility, and facility. For example, the digital ticket by this invention satisfies all the requirements for all the classes of various tickets packed into Table 1 of the conventional technique of drawing 4 . the paper by K.Fuhimura to which Table 1 appeared on World Wide Web in <http://www.w3.org/Dsig/signed-XML99 / pp/NTT#xml#ticket.html> (around the 2000 time), Y.Nakajima, and J.Sekine -- " -- XML Ticket It adopts from; Generalized Ticket Definition Language."

[0193]

As for deformation and adaptation-izing of issue of the digital ticket by this invention, and a digital ticket, according to the above-mentioned explanation, itself will give the design of communication system, and/or the practice person of a code system design technique the hint.

[0194]

for example, meaningful -- it can reach and both unnecessary additional information can be attached to a digital ticket even by the manufacturer, the purchaser, or the porter. furthermore, an exception -- or the fact that both the thing by which different information is also coded, and a non-coded thing will appear on a digital ticket does not become the radical of the obscuration of an essential principle of this invention which carries out a patent claim below

[0195]

For example, the digital signature algorithm with which a secret differs from both a public key is suitable for the use in the digital ticket of this invention.

Similarly, it is not indispensable as an example to print a ticket small or to expropriate easily in a storage. The digital ticket for charged highway passing is printed in 8 1 / 2 "x11" size, is stuck on the aperture of an automobile, and you may enable it to read it by the laser beam in a non-stopped passing-through highway entry tollgate. Or a digital ticket may be loaded in the radio transponder similarly asked in case it is going to ride a vehicle into a charged highway.

[0196]

Furthermore, as already explained, in itself, a digital ticket can also be called cybermoney, an electronic ticket, an electronic coupon, a license, or pass, and does not spoil the essential description again.

[0197]

As for the range of this invention, according to possible deformation and adaptation-izing of these of this invention, and others, it is natural to determine only according to the following claims and not to determine only according to the operation gestalt which taught this invention.

[Brief Description of the Drawings]

[Drawing 1]

Drawing 1 is drawing showing the operation gestalt of the 1st printing paper of the digital ticket by this invention.

[Drawing 2]

Drawing 2 is drawing showing the operation gestalt of the 2nd flexible disk of the digital ticket by this invention.

[Drawing 3]

Drawing 3 is drawing showing the operation gestalt of the 3rd CD-ROM of the digital ticket by this invention.

[Drawing 4]

Drawing 4 is Table 1 of the conventional technique which shows the property of the example of a ticket of a concrete class, and the all are suitable for realizing with the digital ticket by this invention already shown in drawing 1 thru/or drawing 3 .

[Drawing 5]

Drawing 5 is the mimetic diagram of the table explaining the outline of the protocol by this invention for distributing a digital ticket, and the accompanying communication link network.

[Drawing 6]

Drawing 6 is a table explaining the outline of the protocol by this invention for inspecting a digital ticket.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] A ticket supplier company is the computerization approach which can be distributed through a communication channel 5 at a ticket consumer about the digital tickets 1, 2, and 3. The digital tickets 1, 2, and 3 are set as the object of return [winning popularity] behind. Computerization distribution of said digital tickets 1, 2, and 3 and the approach of returning The communication channel 5 is led [1st]. From a ticket supplier company's computer to an anticipation ticket consumer The 1st digital data D1 about the occurrence which can distribute a ticket is transmitted. Said anticipation ticket consumer determines to acquire the digital tickets 1, 2, and 3 to said occurrence. In this way, it becomes a ticket consumer. Said communication channel is led to the 2nd. The 2nd digital data D2 including the directions which expect the ticket for said occurrence to said ticket supplier company's computer from said ticket consumer's computer is transmitted. Subsequently It makes it possible to fill said ticket demand. In said ticket supplier company's computer By using a private key s, the digital signature of the 3rd digital data D3 is calculated. This 3rd digital data D3 is a thing about one side or the both sides of said 1st digital data D1 and said 2nd digital data D2. The digital signature of said digital data D3 (i) In generating of said digital signature, the secret signature key s was used by said ticket supplier company's computer, and (ii) -- one side or the both sides of said digital data D1 and D2 was used about the generating -- It is a thing proving having been stored appropriately in [which can be conveyed] a storage. (iii) said digital data D1 and D2 of the object which generated the digital signature of said digital data D3 Are based on said ticket supplier company of said specific digital ticket to said specific occurrence. It becomes the commemoration (memorialization) of specific supply to said ticket consumer. Specify said ticket consumer as a person in the other end of the communication link performed through said communication channel at least, and he is identified. Said digital data D3 which signed is transmitted to said ticket consumer's computer at least from said ticket supplier company's computer through said communication channel the 3rd. To the 1st, by said ticket consumer's computer, in [which can be conveyed / said] a storage Store said digital data D3 which signed at least, and said storage which can be conveyed is changed into the digital tickets 1, 2, and 3 in this way. said digital tickets 1, 2, and 3 with the gestalt of said storage which contains said digital data D3 which signed at least and which can be conveyed It conveys to the specific time amount and the specific location where the specific occurrence which is the purpose which supplied said digital tickets 1, 2, and 3 is performed physically. In order to return a ticket ticket collector in said specific occurrence Said digital tickets 1, 2, and 3 are repaid. Said digital data D3 which signed is read to said ticket ticket collector's computer at least. In said ticket ticket collector's computer Said digital data D3 is reproduced from said digital data D3 which signed, using the digital verification key v corresponding to said ticket supplier company's signature key s. In said ticket ticket collector's computer [whether said digital data D3 can reappear with the verification key v, and] And when it reappears, said digital data D3 is based on said ticket supplier company of said 3rd specific digital data D3 for said specific occurrence. It judges whether said specific supply to said specific ticket consumer who communicated once through said communication channel is memorized correctly. Although said digital tickets 1, 2, and 3 were confirmed and said digital data D3

was reproduced by use of said verification key v when having memorized Said reproduced digital data D3 is based on said ticket supplier company of said 3rd specific digital data D3 for said specific occurrence. The digital ticket computerization distribution which repeals said digital tickets 1, 2, and 3 when said specific supply to said specific ticket consumer who communicated once through said communication channel is memorized to incorrectness, and the approach of returning.

[Claim 2] In the digital ticket computerization distribution by claim 1, and the approach of returning Said 2nd communication link It is carried out about the 2nd digital data D2 containing the one-way function hash of several R (R). This number R Only said ticket consumer's computer is known and said ticket supplier company's computer is not known. Said count in said ticket supplier company's computer Digital signature Sign about said 3rd digital data D3 including the information I about said event which is the purpose which has the one-way function and said ticket of hash (R) (it is carried out about I||hash (R) s) Said 3rd communication link is performed about Sign (s, I||hash (R)). Said 1st storing R attached to Sign (s, I||hash (R)) as said digital tickets 1, 2, and 3, That is, it is carried out about Sign(s, I||hash (R)) ||R. Reading by said ticket ticket collector's computer It is carried out about Sign(s, I||hash (R)) ||R. The reappearance in said ticket ticket collector's computer It is carried out about I||hash (R), hash (R) is given, and both R and hash (R) are calculated. Said decision Furthermore, when this re-calculated hash (R) is equal to hash (R) to which hash (R) about R was re-calculated and said read digital tickets 1, 2, and 3 reproduced it, When not equal to hash (R) which confirmed said digital tickets 1, 2, and 3, and said read digital tickets 1, 2, and 3 reproduced [said hash (R)], The digital ticket computerization distribution processed so that said digital tickets 1, 2, and 3 may be repealed, and the approach of returning.

[Claim 3] In digital ticket computerization distribution and the approach of returning according to claim 2 Said decision Furthermore, when a meaning is shown first said read digital tickets 1, 2, and 3, When said digital tickets 1, 2, and 3 were confirmed and a meaning is not shown first said read digital tickets 1, 2, and 3, The digital ticket computerization distribution processed so that said digital tickets 1, 2, and 3 may be repealed, and the approach of returning.

[Claim 4] In digital ticket computerization distribution and the approach of returning according to claim 2 Said 2nd communication link It is carried out about one-way hash function hash (R) of several R. The count in said ticket supplier company's computer hash (R) It is carried out about digital signature Sign (s, I||hash (R)) about said 3rd digital data D3 including the information I about said event which is the purpose which has a one-way function and said ticket. Said 3rd communication link is performed about Sign (s, I||hash (R)). Said 1st storing R attached to Sign (s, I||hash (R)) as said digital tickets 1, 2, and 3, That is, it is carried out about Sign(s, I||hash (R)) ||R. Reading by said ticket ticket collector's computer It is carried out about Sign(s, I||hash (R)) ||R. The reappearance in said ticket ticket collector's computer It is carried out about I||hash (R), hash (R) is given, and both R and hash (R) are calculated. Said decision Furthermore, when this re-calculated hash (R) is equal to hash (R) to which hash (R) about R was re-calculated and said read digital tickets 1, 2, and 3 reproduced it, When not equal to hash (R) which confirmed said digital tickets 1, 2, and 3, and said read digital tickets 1, 2, and 3 reproduced [said hash (R)], The digital ticket computerization distribution processed so that said digital tickets 1, 2, and 3 may be repealed, and the approach of returning.

[Claim 5] In digital ticket computerization distribution and the approach of returning according to claim 4 Said decision Furthermore, when a meaning is shown first said read digital tickets 1, 2, and 3, When said digital tickets 1, 2, and 3 were confirmed and a meaning is not shown first said read digital tickets 1, 2, and 3, The digital ticket computerization distribution processed so that said digital tickets 1, 2, and 3 may be repealed, and the approach of returning.

[Claim 6] In digital ticket computerization distribution and the approach of returning according to claim 1 Said count of a digital signature is performed about the digital signature suitable for displaying as a 2-D code. The 1st storing using said ticket consumer's computer is the digital ticket computerization distribution and the approach of returning by printing of said 2-D code 11 to the storage top which can be conveyed [which can be printed].

[Claim 7] It is digital ticket computerization distribution and the approach of returning that said reading

by the computer of said ticket ticket collector of said digital signature is performed using an optical reader in digital ticket computerization distribution and the approach of returning according to claim 6.
[Claim 8] A ticket supplier company is the computerization approach which can be distributed through a communication channel 5 at a ticket consumer about a digital ticket. The communication channel 5 is led [1st]. From a ticket supplier company's computer to an anticipation ticket consumer The data about the occurrence which can distribute a ticket are transmitted. Said anticipation ticket consumer It determines to acquire the digital ticket to the occurrence which specification chose, and becomes a ticket consumer in this way. It sets to said ticket consumer's computer the 1st. Several R is calculated. It sets to said ticket consumer's computer the 2nd. The one-way function of said number R is calculated as hash (R). Said communication channel 5 is led to the 2nd. From said ticket consumer's computer to said ticket supplier company's computer as ticket ordering data Said hash (R) is transmitted at least and, subsequently it makes it possible to fill said ticket demand. It sets to said ticket supplier company's computer the 3rd. The digital signature of hash (R) attached to the information I about said event about the signature key s Calculate as Sign (s, I||hash (R)) and this Sign (s, I||hash (R)) constitutes the digital ticket antecedent. Said communication channel is led to the 3rd. From said ticket supplier company's computer to said ticket consumer's computer Said digital ticket antecedent Sign (s, I||hash (R)) is transmitted. It sets to said ticket consumer's computer the 4th. As attachment to said digital ticket antecedent Sign of R (s, I||hash (R)) Sign(s, I||hash (R)) ||R is calculated as digital tickets 1, 2, and 3. The digital ticket computerization distribution which stores said digital ticket Sign(s, I||hash (R)) ||R in the storage which can be conveyed from said ticket consumer's computer the 1st, and the approach of returning.
[Claim 9] Are an approach according to claim 8, and it expands and extends to use of said digital ticket by said ticket consumer in the event which said specification chose. After said writing and said approach are . Said storage which wrote in said digital tickets 1, 2, and 3 containing Sign(s, I||hash (R)) ||R and which can be conveyed It conveys to the event which said specification chose. Said digital tickets 1, 2, and 3 in [which can be conveyed / said] a storage are repaid and verified. The event which said specification chose is entered. Sign(s, I||hash (R)) ||R of said digital tickets 1, 2, and 3 is read into an event computer. from said read Sign(s, I||hash (R)) ||R Said number R is extracted to said event computer. To the 5th, I||hash (R) is calculated using said signature key s and the complementary verification key v. It sets to said event computer the 6th. hash (R) is calculated using the same one-way function before used in said 2nd count. Subsequently, hash (R) by R and the 6th count is calculated. hash (R) by said 6th count is compared with the hash (R) part of I||hash (R) by said 5th count. Said 5th count is processed correctly and said information I is right to said event. When hash (R) by said 6th count is equivalent to hash (R) by count of the 5th of said read digital ticket, [whether said 5th count is correctly processed by permitting the holder of said digital tickets 1, 2, and 3 entrance, and] Or when hash (R) said information I is not right to said event, or according to said 6th count is not equivalent to hash (R) by said count of the 5th of said read digital tickets 1, 2, and 3, How to refuse entrance to the holder of said digital tickets 1, 2, and 3.
[Claim 10] In an approach according to claim 9, said 5th count is processed correctly, and said information I is right to said event. hash (R) by said 6th count is equivalent to hash (R) by count of the 5th of said read digital ticket. When a meaning is shown first said read digital tickets 1, 2, and 3, [whether said 5th count is correctly processed by permitting the holder of said digital tickets 1, 2, and 3 entrance, and] Or said information I is not right to said event, or hash (R) by said 6th count is not equivalent to hash (R) by said count of the 5th of said read digital tickets 1, 2, and 3. Or the method of refusing entrance to the holder of said digital tickets 1, 2, and 3, when a meaning is not shown first said read digital tickets 1, 2, and 3.
[Claim 11] It sets to an approach according to claim 9, and is between said extract and said 5th count. How to include storing R in said event computer the 2nd as directions with which said digital tickets 1, 2, and 3 were repaid.
[Claim 12] In an approach according to claim 8 Said ticket supplier company is also a ticket vender, said ticket consumer is also a purchaser of a ticket, and distribution to said ticket consumer of said ticket

which led said communication channel is accompanied by sale of said digital tickets 1, 2, and 3. Said 2nd transmission is an approach including the electronic payment suitable for said ordering data.
[Claim 13] In an approach according to claim 8 Said 1st transmission, said 2nd transmission, and said 3rd transmission are the approach of performing on the communication network 5 which reaches all over the world.
[Claim 14] In an approach according to claim 8 Said 1st transmission, said 2nd transmission, and said 3rd transmission are the approach of performing on the safe communication network 5 of a worldwide scale in a code.
[Claim 15] In an approach according to claim 14 Said 1st transmission, said 2nd transmission, and said 3rd transmission are the approach of performing on the Internet.
[Claim 16] In an approach according to claim 15 Said 1st transmission, said 2nd transmission, and said 3rd transmission are the approach of performing on the secure sockets layer (namely, SSL) of the Internet.
[Claim 17] In an approach according to claim 8 It is the approach which then, performs said 1st storing in the medium which can be conveyed, can distribute to the site of the event which said specification chose behind physically, and is repaid by said ticket consumer as digital tickets 1, 2, and 3 to it.
[Claim 18] In an approach according to claim 8 Said 1st storing is performed in said medium of the printed substrate which can be conveyed. Said printed encryption digital record is an approach which then, can distribute to the site of the event which said specification chose behind physically, and is repaid by said ticket consumer as said digital ticket to it.
[Claim 19] In an approach according to claim 18 Said 1st storing in said medium of a printing substrate which can be conveyed is the approach of being the gestalt of a two dimensions bar code 11.
[Claim 20] In an approach according to claim 19 Said 1st storing in said medium of the printed two dimensions bar code 11 which can be conveyed is the approach of performing according to PDF417 specification.
[Claim 21] In an approach according to claim 19 Said 1st storing in said medium of the printed two dimensions bar code 11 which can be conveyed is the approach of performing according to QR specification.
[Claim 22] In an approach according to claim 8 The 1st storing in said medium which can be conveyed is the approach of performing about the computer disks 2 and 3.
[Claim 23] In an approach according to claim 8 Said 1st storing is performed in said medium of a smart card which can be conveyed. Said digital record stored in said smart card is the approach of then, distributing to the site of the event which said specification chose behind physically, and repaying as said digital ticket by said ticket consumer to it.
[Claim 24] It is the system which distributes a digital ticket on a communication network. Ticket ordering data is transmitted to a ticket supplier company's computer on said communication network the 1st. To the 1st, on said communication network 5, from said ticket supplier company's computer The ticket data by which the digital signature was carried out are received. Since said ticket data by which the digital signature was carried out are stored in the storage which can be conveyed A ticket consumer's computer linked to said communication network 5, The ticket ordering data transmitted to the 2nd from said ticket consumer's computer on said communication network 5 said 1st [the] is received. Said ticket data are signed in digital one. In order to transmit said ticket data which signed in digital one to said ticket consumer's computer on said communication network 5 the 2nd, A ticket supplier company's computer linked to said communication network, To the 1st time, said transmission of the 1st of said ticket consumer's computer It transmits to said reception of the 2nd of said ticket supplier company's computer. In order to transmit said transmission of the 4th of said ticket supplier company's computer to said reception of the 1st of said ticket consumer's computer at the 2nd time System equipped with a communication network.,
[Claim 25] In a digital ticket distribution system according to claim 24 Said ticket consumer's computer Several R is calculated to the 1st. The one-way function of R is calculated and hash (R) is calculated [2nd] as ticket data. Said 1st transmission It carries out about hash (R) calculated to said 2nd [the] as

said ticket data. Said 1st reception About hash (R) and the additional information I that it signed in digital one using the signature key s It carries out as Sign (s, I||hash (R)). Attachment is calculated [3rd] to said digital ticket antecedent Sign of R (s, I||hash (R)). Sign(s, I||hash (R)) ||R is given as a digital ticket. Said storing It carries out about digital ticket Sign(s, I||hash (R)) ||R calculated to said 3rd [the]. Said ticket supplier company's computer The hash(R) ticket ordering data transmitted to the 2nd said 1st [the] is received. Said ticket data and the digital signature about the additional information I are related with the signature key s. It calculates as Sign (s, I||hash (R)). Digital ticket distribution system which transmits said calculated Sign (s, I||hash (R)) to the 2nd.

[Claim 26] In a digital ticket distribution system according to claim 25 Said ticket consumer's computer is a digital ticket distribution system which stores this by printing said digital ticket.

[Claim 27] In a digital ticket distribution system according to claim 26 Said ticket consumer's computer is a digital ticket distribution system which stores this by printing said digital ticket to the pattern which can be 2-D machine read.

[Claim 28] In a digital ticket distribution system according to claim 27 Said ticket consumer's computer is a digital ticket distribution system which stores this by printing said digital ticket to the bar code pattern which can be 2-D machine read.

[Claim 29] It is the system which distributes a digital ticket on a communication network. Several R is calculated to the 1st. The one-way function of R is calculated [2nd]. hash (R) is calculated as ticket data. hash (R) calculated said 2nd [the] to a ticket supplier company's computer on said communication network 5 the 1st It transmits as ticket data for the event which specification chose. To the 1st The data about the signature key s of hash (R) and the additional information I which signed in digital one It receives as Sign (s, I||hash (R)). Attachment is calculated [3rd] to said digital ticket antecedent Sign of R (s, I||hash (R)). Sign(s, I||hash (R)) ||R is given as a digital ticket. Since digital ticket Sign(s, I||hash (R)) ||R calculated to the 1st said 3rd [the] is stored in the storage which can be conveyed a ticket consumer's computer linked to a communication network 5, The hash(R) ticket data transmitted to the 2nd from said ticket consumer's computer on said communication network said 1st [the] are received. The data about the signature key s of hash (R) which received to the 4th the 2nd, and Information I which signed in digital one are calculated as Sign (s, I||hash (R)). To the 2nd, on said communication network 5 In order to transmit Sign (s, I||hash (R)) calculated to said 4th [the] to said ticket consumer's computer A ticket supplier company's computer linked to said communication network 5, To the 1st time, said transmission of the 1st of said ticket consumer's computer It transmits to said reception of the 2nd of said ticket supplier company's computer. In order to transmit said transmission of the 4th of said ticket supplier company's computer to said reception of the 1st of said ticket consumer's computer at the 2nd time System equipped with a communication network 5.,

[Claim 30] It is a digital ticket. Digital ticket containing the digital signature of the publisher of a ticket which consists of the data carrier which can be conveyed [material].

[Claim 31] In a digital ticket according to claim 30 said data carrier which can be conveyed [material] R is said ticket consumer's secret random number including Sign(s, I||hash (R)) ||R. hash (R) is a digital ticket which is a digital signature about the signature key s with said ticket supplier company of said hash (R) which attached Sign (s, I||hash (R)) to Information I are the one-way function of R and secret.

[Claim 32] It is the digital ticket supplied by the ticket consumer by bidirectional processing with this from the ticket supplier company on the communication network. It has the data carrier containing Sign (s, I||hash (R)) ||R which can be conveyed [material]. R is said ticket consumer's secret random number, and hash (R) is the one-way function of R. Sign (s, I||hash (R)) The digital ticket which is a digital signature about said ticket supplier company's secret signature key s of said hash (R) attached to Information I.

[Claim 33] It is the digital ticket supplied by the ticket consumer by bidirectional processing with a ticket supplier company on the communication network. It has the data carrier containing Sign(s, I||hash (R)) ||R which can be conveyed [material]. (1) R It is the number which has the origin in said ticket consumer's computer. this -- several R (2) several -- Sign (s, I||hash (R)) -- attaching -- several [this] -- Sign (s, I||hash (R)) The data which signed in digital one in said ticket supplier company's computer

about a number hash (R) of signature keys s attached to Information I, It calculates as Sign (s, I||hash (R)), and transmits to said ticket consumer's computer through said communication network 5 later. Namely, said number hash (R) In said ticket supplier-company consumer's computer, it is calculated as a one-way function of R in itself. It is later transmitted to said ticket supplier company's computer. Number R It has the origin in said ticket consumer's computer, is said ticket consumer's secret, and is not public. Said digital signature key s of said ticket supplier company's computer is said ticket supplier company's secret, and is a digital ticket which is not public.

[Claim 34] It is a digital ticket. It consists of the digital data storage which can be conveyed [material]. This digital data storage that can be conveyed [material] It is known by both the purchaser of a ticket, and the vender from the first. The 1st sort data which are meaningful in order to identify relatively at least the specific event which is the purpose which sold said ticket for the vender of said ticket, The 2nd sort data containing the digital representation with a signature of the specific parameter which the computer generated one by one from the first are included. To the 1st, by the purchaser of said ticket As an irreversible function of the random number called "the irreversible function made first", subsequently By the vender of said ticket, as a digital signature of the irreversible function made by the 2nd at said beginning subsequently The purchaser of said ticket attaches the same random number to the 3rd. In order for said ticket to win popularity and to judge the effectiveness of said digital ticket at the time of return trial Said random number is taken out. The irreversible function made by said the 1st time which signed is interpreted. The irreversible function made by the 1st time of this is reproduced. The irreversible function of the same thing as said taken-out random number is newly made again. this -- the newly made irreversible function -- "the irreversible function made by the 2nd time" and a call -- When the irreversible function made by said the 2nd time is equal to the irreversible function made by said the 1st time, Said ticket is a digital ticket which repeals said digital ticket to said specific event at least when it is not invalid and the irreversible function made by said the 2nd time is not equal to the irreversible function made by said the 1st time.

[Claim 35] The digital ticket performed for the statistical purpose in order to judge whether they are whether the digital ticket to which the comparison with the database of the digital ticket which it was further actually signed and was sold in the digital ticket according to claim 34 in said digital signature in said material medium which the digital reader read was repaid is effective, and an invalid.

[Claim 36] The digital ticket whose digital signature in said material medium is visible in a digital ticket according to claim 34.

[Claim 37] In a digital ticket according to claim 34 The digital signature which is visible to said eye is a digital ticket which judges whether the repaid digital ticket is effective or invalid by [of the digital ticket which it was actually signed and was sold by the eye] performing the comparison with the catalog of a detectable expression visually.

[Claim 38] It is the system which distributes a digital ticket to the purchaser of a ticket from a ticket vender. It is communication channel. To the 1st time, from a ticket vender to the purchaser of a ticket It is delivery about the data about an event to have a ticket. To the 2nd time A number of irreversible data representation determined as said ticket vender only by the purchaser of said ticket from the purchaser of said ticket Delivery, The digital signature of said irreversible conversion from said ticket vender to the purchaser of said ticket at the 3rd time Delivery, The communication channel which manufactures a digital ticket for the digital signature which said irreversible conversion received combining said number, Connect with said communication channel in the state of a communication link, and the number of (i) above is determined. (ii) The computer of the purchaser of a ticket who calculates said irreversible conversion and creates a digital ticket for said (iii) irreversible conversion combining said number, Connect with said communication channel in the state of a communication link, and it is related with the irreversible conversion received from said purchaser. The computer of the ticket vender who calculates the digital signature of this irreversible conversion, Connect with said purchaser's computer and said digital ticket is stored. A digital ticket distribution system equipped with the material portable medium for conveying this digital ticket to the physical site of the event which the specification which can use it for entrance chose.

[Claim 39] It is the system by which said communication channel sends a random number to the 2nd time in a system according to claim 38.
[Claim 40] It is the system which sends the number showing the event from which said specification chose said communication channel as the 2nd time in the system according to claim 38.
[Claim 41] It sets to a system according to claim 38, and is said communication channel. System equipped with the digital communication network of a worldwide scale.
[Claim 42] It is a system equipped with the digital communication network where said communication channel is safe for a worldwide scale in a system according to claim 38.
[Claim 43] It is the system by which said digital data storing concreteness portable medium consists of a computer disk in a system according to claim 38.
[Claim 44] It is the system by which said digital data storing concreteness portable medium consists of print media in a system according to claim 38.
[Claim 45] The printing ticket support index that it is a printing ticket support index, and it is characterized by including the 2-D bar code which can judge the justification of said ticket and which includes all required information absolutely even if this index is not a meaning.
[Claim 46] It is the printing ticket support index characterized by including the data with which said 2-D bar code-like index was further signed by the supplier company of said ticket in digital one in the printing ticket support index according to claim 45.
[Claim 47] It is the printing ticket support index characterized by including a number of one-way functions with which said 2-D bar code-like index is given by the holder of said ticket in a printing ticket support index according to claim 45.
[Claim 48] In a printing ticket support index according to claim 45 further said 2-D bar code-like index Sign(s, I||hash (R)) ||R is included. (1) R It is the number which has the origin in said ticket consumer's computer. this -- several R (2) several -- Sign (s, I||hash (R)) -- attaching -- several [this] -- Sign (s, I||hash (R)) In the computer of the supplier company of said ticket, it is calculated as a digital signature about a number hash (R) of digital signature keys s combined with Information I. It transmits to said ticket consumer's computer through said communication network after . Said number hash (R) Itself In said ticket supplier-company consumer's computer It is calculated as a one-way function of R, and is later transmitted to said ticket supplier company's computer. Number R It has the origin in said ticket consumer's computer, is said ticket consumer's secret, and is not public. Said digital signature key s of said ticket supplier company's computer The printing ticket support index which is said ticket supplier company's secret and is characterized by what is not public.
[Claim 49] It is the communication system which sells and distributes a digital ticket. (i) One direction conversion of a secret number to a vender's computer at the 1st time Delivery, (ii) To the 3rd time, information with a signature is received from said ticket vender's computer. Said received encryption signature information to the 4th (iii) time with said secret number The computer of the purchaser of a ticket who stores in a digital store, (i) To the 1st time, one direction conversion of said private key from said vender's computer is received. (ii) This one direction conversion and additional information are signed at the 2nd time. Said 1st conversion and additional information that it signed, to the 3rd (iii) time as information that it signs A ticket seller's computer sent to the computer of the purchaser of said ticket, It has the digital store which stores in the 4th time said information that it signs and said secret number, as a digital ticket. (i) When reading said information that it signs, (ii) When decoding said information that it signs and reproducing one direction conversion of said secret number, When reproducing again the 1st same safe conversion as said vender used for the 1st safe conversion of said number, (iii) and (iv) -- the communication system which can attain effectiveness decision of said digital ticket when comparing said decoded reappearance one direction conversion with said 1st reproduced conversion.
[Claim 50] It is the approach of selling and distributing a digital ticket. As the 1st time To a ticket vender's computer, set one direction conversion of a secret number as the 1st transmission from the computer of the purchaser of a ticket, and one direction conversion of said secret number is set to said ticket seller's computer as delivery and the 1st time. It receives as the 1st reception. As the 2nd time, said one direction information and additional information are signed in said ticket vender's computer. As

the 3rd time To the computer of the purchaser of said ticket, from said ticket vender's computer, as information that it signs Considering said 1st conversion and additional information that it signed, as the 2nd transmission, it is delivery. As the 3rd time, said information that it signs is set to the computer of the purchaser of said ticket. It receives as the 2nd reception. The information that it signs and the (ii) aforementioned secret number which carried out the (i) aforementioned reception are stored in a digital memory store, using the computer of the purchaser of said ticket as the 4th time. As the 4th time Said information that it signs and said secret number are stored in said digital memory store as a digital ticket. (i) When reading said information that it signs, (ii) When decoding said information that it signs and reproducing one direction conversion of said secret number, When reproducing again to the 1st safe conversion of said number using the 1st safe conversion of same 45 as said vender used, (iii) and (iv) -- the approach that effectiveness decision of said digital ticket can be attained when comparing said decoded reappearance one direction conversion with said 1st reproduced conversion.

[Claim 51] In the communication system which has the computer of the purchaser of a ticket who performs two-way communication to a ticket seller's safe computer through a non-insurance digital communication network It is the approach of selling and distributing a digital ticket to the purchaser of a ticket from a ticket seller. As the 1st time The 1st data about the event which is the purpose which has a ticket from said ticket seller's computer to the computer of the purchaser of said ticket is sent as the 1st transmission through said communication network. Subsequently As the 2nd time Said communication network is led. From said ticket seller's computer The 2nd data which identifies the event which asks for a ticket to the computer of the purchaser of said ticket as the 2nd transmission to delivery and said 2nd data It is determined by only the ticket purchaser and the 1st safe conversion of the number which is not known is made to accompany the person of others including said ticket vender. Said communication network is led. From said ticket seller's computer The 3rd data which checks issue of the ticket to the event which asks for said ticket to the computer of the purchaser of said ticket as the 3rd transmission to delivery and this 3rd data The 2nd safe conversion of said 1st safe conversion is made to accompany. The computer of the purchaser of said ticket is used. the inside of the material portable medium of digital data storage -- (ii) -- (i) accompanied by said 2nd safe conversion -- said number -- storing -- (i) -- at the time of transportation to the physical site of said event of said digital data storing medium (ii) by use of the 1st same safe conversion as said purchaser used When reading said number into a computer and reproducing the 1st safe conversion of said number again, It reaches. (iii) When the event computer which has the privilege of getting to know said 2nd conversion reverses said 2nd safe conversion, (ii) How to enable effectiveness decision of said digital ticket as compared with the 1st conversion which reproduced the 1st conversion of which reading playback was done by performing said (iii) 2nd conversion conversely.

[Claim 52] It is the approach of performing about said 2nd data accompanied by the 1st conversion with the gestalt of the one-way hash function of said number safe for said 2nd transmission in an approach according to claim 51.

[Claim 53] It is the approach of performing about said 2nd data accompanied by conversion with the gestalt of the digital signature of said 1st safe conversion safe for said 3rd transmission in an approach according to claim 51.

[Claim 54] It is the approach storing into the material portable medium of digital data storage consists of printing in an approach according to claim 51.

[Claim 55] It is the approach of performing said printing at least in an approach according to claim 51 about said 2nd safe conversion of the gestalt of the (ii) two dimensions bar code.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2003－501712
（P2003－501712A）
(43)公表日　平成15年１月14日(2003.1.14)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　17/60	４１０	Ｇ０６Ｆ　17/60	４１０Ａ　５Ｊ１０４
	５１２		５１２
	ＺＥＣ		ＺＥＣ
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ

審査請求　未請求　予備審査請求　有　（全 87 頁）

(21)出願番号　特願2001－500482(P2001－500482)
(86)（22)出願日　平成12年５月30日(2000.5.30)
(85)翻訳文提出日　平成13年12月３日(2001.12.3)
(86)国際出願番号　ＰＣＴ／ＵＳ００／１４９１５
(87)国際公開番号　ＷＯ００／０７４３００
(87)国際公開日　平成12年12月７日(2000.12.7)
(31)優先権主張番号　６０／１３７，０２７
(32)優先日　平成11年６月１日(1999.6.1)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０９／４９０，３５４
(32)優先日　平成12年１月24日(2000.1.24)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　ザ・リージェンツ・オブ・ザ・ユニバーシティ・オブ・カリフォルニア
アメリカ合衆国カリフォルニア州94612，オークランド，レイクサイド・ドライブ300，トゥエンティファースト・フロア
(72)発明者　古林　紀哉
岡山県倉敷市福島406番地の５
(72)発明者　イー，ベネット
アメリカ合衆国カリフォルニア州92009，カールズバッド，フリムベル・コート995
(74)代理人　弁理士　社本　一夫　（外４名）

Ｆターム(参考)　5J104 AA09 LA05 LA06 NA02 PA07 PA12

(54)【発明の名称】　ディジタル・チケットの配信および検査システムおよび方法

(57)【要約】
好ましくは、インターネット上で、消費者が供給業者からディジタル・チケット（１）を調達する。ディジタル・チケット（１）は、通常、消費者が紙に印刷した２－Ｄバーコード（１１）の形態の有形輸送可能データ媒体内、あるいは消費者の可搬性ディスク、ＣＤ－ＲＯＭまたはスマート・メディア上に具体化されることになる。チケットを発生するには、消費者が数Ｒを選択し、hash(R)を供給業者に送る。供給業者は、チケットに関連する、選択されたサービスに関する情報をhash(R)に連携し、その結果に署名し、Sign(s,Ihash(R))を消費者に送る。すると、消費者はＲを連携して、チケットの一部として、Sign(s,Ihash(R))Rを形成する。使用するには、チケットを、物理的媒体内で、受け戻し点に輸送し、提示する。供給業者の秘密鍵を用いてイベントに関する情報、およびhash(R)を再現することによって、検証を行う。次いで、Ｒをハッシュし、比較して、チケットの正当性を証明する。

ら前記チケット 消費者のコンピュータに少なくとも前記署名したディジタル・データD_3を伝達し、

第1 に、前記チケット 消費者のコンピュータによって、前記輸送可能記憶媒体内に、少なくとも前記署名したディジタル・データD_3を格納し、こうして前記輸送可能記憶媒体をディジタル・チケット１、２、３に変換し、

前記ディジタル・チケット１、２、３を、少なくとも前記署名したディジタル・データD_3を含むような前記輸送可能記憶媒体の形態で、前記ディジタル・チケット１、２、３を供給した目的である特定の出来事が行われる特定の時間および場所に、物理的に輸送し、

前記特定の出来事においてチケット 集札係に受け戻すために、前記ディジタル・チケット１、２、３を弁済し、

少なくとも前記署名したディジタル・データD_3を、前記チケット 集札係のコンピュータに読み取り、

前記チケット 集札係のコンピュータにおいて、前記チケット 供給業者の署名鍵s に対応するディジタル検証鍵v を用いて、そして前記署名したディジタル・データD_3から、前記ディジタル・データD_3を再現し、

前記チケット 集札係のコンピュータにおいて、前記ディジタル・データD_3が検証鍵v によって再現可能であるか、そして再現された場合に、前記ディジタル・データD_3が、前記特定の出来事のための前記特定の第3 ディジタル・データD_3の前記チケット 供給業者による、前記通信チャネルを通じて一度通信した前記特定のチケット 消費者への前記特定の供給を正しく記憶しているか判定し、記憶している場合、前記ディジタル・チケット１、２、３を有効であるとし、前記ディジタル・データD_3が前記検証鍵v の使用によって再現されたが、前記再現されたディジタル・データD_3が、前記特定の出来事のための前記特定の第3 ディジタル・データD_3の前記チケット 供給業者による、前記通信チャネルを通じて一度通信した前記特定のチケット 消費者への前記特定の供給を不正確に記憶している場合、前記ディジタル・チケット１、２、３を無効とする、

ディジタル・チケット・コンピュータ化配信および受け戻し方法。

【 請求項2 】　請求項1 によるディジタル・チケット・コンピュータ化配信

および受け戻し方法において、

前記第２の通信は、数Ｒの一方向ハッシュ関数hash(R)について行われ、

前記チケット供給業者のコンピュータにおける計算は、hash(R)の一方向関数および前記チケットを有する目的である前記イベントに関する情報Ｉを含む前記第３ディジタル・データD_3に関するディジタル署名Sign(s,I||hash(R))について行われ、

前記第３の通信は、Sign(s,I||hash(R))について行われ、

前記第１の格納は、前記ディジタル・チケット１、２、３としての、Sign(s,I||hash(R))に添付したＲ、即ち、Sign(s,I||hash(R))||Rについて行われ、

前記チケット集札係のコンピュータへの読み取りは、Sign(s,I||hash(R))||Rについて行われ、

前記チケット集札係のコンピュータにおける再現は、I||hash(R)について行われ、hash(R)を与え、Ｒおよびhash(R)双方を求め、

前記決定は、更に、Ｒに関するhash(R)を再計算し、該再計算したhash(R)が前記読み取ったディジタル・チケット１、２、３の再現したhash(R)に等しい場合、前記ディジタル・チケット１、２、３を有効とし、前記hash(R)が前記読み取ったディジタル・チケット１、２、３の再現したhash(R)に等しくない場合、前記ディジタル・チケット１、２、３を無効とするように処理する、

ディジタル・チケット・コンピュータ化配信および受け戻し方法。

【請求項５】　請求項４記載のディジタル・チケット・コンピュータ化配信および受け戻し方法において、

前記決定は、更に、前記読み取ったディジタル・チケット１、２、３が最初に一意に提示された場合、前記ディジタル・チケット１、２、３を有効とし、前記読み取ったディジタル・チケット１、２、３が最初に一意に提示されたのではない場合、前記ディジタル・チケット１、２、３を無効とするように処理する、

ディジタル・チケット・コンピュータ化配信および受け戻し方法。

【請求項６】　請求項１記載のディジタル・チケット・コンピュータ化配信および受け戻し方法において、

ディジタル署名の前記計算は、２－Ｄコードとして表示するのに適したディジ

チケット 先行物Sign(s,I||hash(R))への添付として、Sign(s,I||hash(R))||Rをディジタル・チケット１、２、３として計算し、

第1 に、前記ディジタル・チケットSign(s,I||hash(R))||Rを、前記チケット消費者のコンピュータから輸送可能記憶媒体に格納する、

ディジタル・チケット・コンピュータ化配信および受け戻し方法。

【 請求項9 】 請求項8 記載の方法であって、前記特定の選択したイベントにおいて前記チケット 消費者による前記ディジタル・チケット の使用に拡大かつ拡張し、前記書き込みの後、前記方法は、更に、

Sign(s,I||hash(R))||Rを含む前記ディジタル・チケット１、２、３ を書き込んだ前記輸送可能記憶媒体を、前記特定の選択したイベント に輸送し、

前記輸送可能記憶媒体内の前記ディジタル・チケット１、２、３ を弁済し、検証して、前記特定の選択したイベント に入場し、

前記ディジタル・チケット１、２、３ のSign(s,I||hash(R))||Rをイベント・コンピュータに読み込み、

前記読み込んだSign(s,I||hash(R))||Rから、前記数R を前記イベント・コンピュータに抽出し、

第5 に、前記署名鍵s と相補的な検証鍵v を用いてI||hash(R)を計算し、

第6 に、前記イベント・コンピュータにおいて、前記第2 の計算において以前に用いた同じ一方向関数を用いて、hash(R)を計算し、次いでR および第6 の計算によるhash(R)を求め、

前記第6 の計算によるhash(R)を前記第5 の計算によるI||hash(R)のhash(R)部分と 比較し、

前記第5 の計算が正しく 処理され、前記情報I が前記イベント に対して正しく、前記第6 の計算によるhash(R)が前記読み取ったディジタル・チケット の第5 の計算によるhash(R)に相当する場合、前記ディジタル・チケット１、２、３ の保持者に入場を許可し、前記第5 の計算が正しく 処理されないか、あるいは前記情報I が前記イベント に対して正しくないか、あるいは前記第6 の計算によるhash(R)が前記読み取ったディジタル・チケット１、２、３ の前記第5 の計算によるhash(R)に相当しない場合、前記ディジタル・チケット１、２、３ の保持者に

全である、世界規模の通信ネットワーク５上で行う、方法。

【請求項１５】　請求項１４記載の方法において、

前記第１の送信、前記第２の送信、および前記第３の送信は、インターネット上で行う、方法。

【請求項１６】　請求項１５記載の方法において、

前記第１の送信、前記第２の送信、および前記第３の送信は、インターネットのセキュア・ソケット・レイヤ（即ちＳＳＬ）上で行う、方法。

【請求項１７】　請求項８記載の方法において、

前記第１の格納は、輸送可能媒体において行い、後に前記特定の選択したイベントのサイトに物理的に配信可能であり、そこで前記チケット消費者によってディジタル・チケット１、２、３として弁済される、方法。

【請求項１８】　請求項８記載の方法において、

前記第１の格納は、印刷した基板の前記輸送可能媒体において行い、

前記印刷した暗号化ディジタル・レコードは、後に前記特定の選択したイベントのサイトに物理的に配信可能であり、そこで前記チケット消費者によって前記ディジタル・チケットとして弁済される、方法。

【請求項１９】　請求項１８記載の方法において、

印刷基板の前記輸送可能媒体における前記第１の格納は、二次元バーコード１１の形態である、方法。

【請求項２０】　請求項１９記載の方法において、

印刷した二次元バーコード１１の前記輸送可能媒体における前記第１の格納は、ＰＤＦ４１７規格にしたがって行う、方法。

【請求項２１】　請求項１９記載の方法において、

印刷した二次元バーコード１１の前記輸送可能媒体における前記第１の格納は、ＱＲ規格にしたがって行う、方法。

【請求項２２】　請求項８記載の方法において、

前記輸送可能媒体における第１の格納は、コンピュータ・ディスク２、３について行う、方法。

【請求項２３】　請求項８記載の方法において、

第2に、Rの一方向関数を計算して、チケット・データとしてhash(R)を求め、

前記第1の送信は、前記チケット・データとしての、前記第2に計算したhash(R)について行い、

前記第1の受信は、署名鍵sを用いてディジタル的に署名したhash(R)および追加情報Iについて、Sign(s,I||hash(R))として行い、

第3に、Rの前記ディジタル・チケット先行物Sign(s,I||hash(R))へ添付を計算して、Sign(s,I||hash(R))||Rをディジタル・チケットとして与え、前記格納は、前記第3に計算したディジタル・チケットSign(s,I||hash(R))||Rについて行い、

前記チケット供給業者のコンピュータは、

第2に、前記第1に送信したhash(R)チケット発注データを受信し、

前記チケット・データおよび追加情報Iに関するディジタル署名を、署名鍵sに関して、Sign(s,I||hash(R))として計算し、

第2に、前記計算したSign(s,I||hash(R))を送信する、

ディジタル・チケット配信システム。

【請求項26】　請求項25記載のディジタル・チケット配信システムにおいて、

前記チケット消費者のコンピュータは、前記ディジタル・チケットを印刷することによって、これを格納する、ディジタル・チケット配信システム。

【請求項27】　請求項26記載のディジタル・チケット配信システムにおいて、

前記チケット消費者のコンピュータは、前記ディジタル・チケットを2－D機械読み取り可能パターンに印刷することによって、これを格納する、ディジタル・チケット配信システム。

【請求項28】　請求項27記載のディジタル・チケット配信システムにおいて、

前記チケット消費者のコンピュータは、前記ディジタル・チケットを2－D機械読み取り可能バー・コード・パターンに印刷することによって、これを格納す

を備えるシステム。

【請求項３０】　ディジタル・チケットであって、

チケットの発行者のディジタル署名を含む、有形輸送可能データ記憶媒体から成るディジタル・チケット。

【請求項３１】　請求項３０記載のディジタル・チケットにおいて、前記有形輸送可能データ記憶媒体は、Sign(s,I||hash(R))||Rを含み、Rは前記チケット消費者の秘密の乱数であり、hash(R)はRの一方向関数であり、Sign(s,I||hash(R))は、情報Iに添付した前記hash(R)の、前記チケット供給業者の秘密の署名鍵sに関するディジタル署名である、ディジタル・チケット。

【請求項３２】　通信ネットワーク上において、チケット供給業者からおよびこれとの双方向処理によってチケット消費者によって調達したディジタル・チケットであって、

Sign(s,I||hash(R))||Rを含む有形輸送可能データ記憶媒体を備え、Rは前記チケット消費者の秘密の乱数であり、hash(R)はRの一方向関数であり、Sign(s,I||hash(R))は、情報Iに添付した前記hash(R)の、前記チケット供給業者の秘密の署名鍵sに関するディジタル署名である、ディジタル・チケット。

【請求項３３】　通信ネットワーク上において、チケット供給業者との双方向処理によってチケット消費者によって調達したディジタル・チケットであって、

Sign(s,I||hash(R))||Rを含む有形輸送可能データ記憶媒体を備え、

（１）Rは、前記チケット消費者のコンピュータ内にその起源を有する数であり、該数Rを、

（２）数Sign(s,I||hash(R))に添付し、該数Sign(s,I||hash(R))は、前記チケット供給業者のコンピュータにおいて、情報Iに添付した数hash(R)の署名鍵sに関してディジタル的に署名したデータ、即ち、Sign(s,I||hash(R))として計算し、後に前記通信ネットワーク５を通じて前記チケット消費者のコンピュータに伝達し、前記数hash(R)は、それ自体、前記チケット供給業者消費者のコンピュータにおいて、Rの一方向関数として計算され、後に前記チケット供給業者のコンピュータに伝達されたものであり、

対して前記ディジタル・チケットを無効とする、

ディジタル・チケット。

【請求項35】　請求項34記載のディジタル・チケットにおいて、ディジタル・リーダが読み取った、前記有形媒体内の前記ディジタル署名を、更に、実際に署名され販売されたディジタル・チケットのデータベースとの比較を、弁済されたディジタル・チケットが有効かまたは無効かを判定するためではなく、統計的目的で行う、ディジタル・チケット。

【請求項36】　請求項34記載のディジタル・チケットにおいて、前記有形媒体内のディジタル署名が目に見える、ディジタル・チケット。

【請求項37】　請求項34記載のディジタル・チケットにおいて、

前記目に見えるディジタル署名は、目によって、実際に署名され販売されたディジタル・チケットの視覚的に検知可能な表現のカタログとの比較を行うことによって、弁済されたディジタル・チケットが有効かまたは無効かについて判定を行う、ディジタル・チケット。

【請求項38】　チケット販売者からチケットの購入者にディジタル・チケットは配信するシステムであって、

通信チャネルであって、

1回目に、チケット販売者からチケットの購入者に、チケットを有する目的のイベントに関するデータを送り、

2回目に、前記チケットの購入者から前記チケット販売者に、前記チケットの購入者のみによって決定した数の非可逆データ表現を送り、

3回目に、前記チケット販売者から前記チケットの購入者に、前記非可逆変換のディジタル署名を送り、

前記非可逆変換の受信したディジタル署名を、前記数と組み合わせてディジタル・チケットを製作する、通信チャネルと、

前記通信チャネルに、通信状態で接続され、（ｉ）前記数を決定し、（ｉｉ）前記非可逆変換を計算し、（ｉｉｉ）前記非可逆変換を前記数と組み合わせてディジタル・チケットを作成する、チケットの購入者のコンピュータと、

前記通信チャネルに通信状態で接続され、前記購入者から受信した非可逆変換

前記2－Dバーコード状指標は、Sign(s,I||hash(R))||Rを含み、

（1）Rは、前記チケット消費者のコンピュータ内にその起源を有する数であり、該数Rを、

（2）数Sign(s,I||hash(R))に添付し、該数Sign(s,I||hash(R))は、前記チケットの供給業者のコンピュータにおいて、情報Iと組み合わせた数hash(R)のディジタル署名鍵sに関するディジタル署名として計算され、

後に前記通信ネットワークを通じて前記チケット消費者のコンピュータに伝達し、前記数hash(R)は、それ自体、

前記チケット供給業者消費者のコンピュータにおいて、Rの一方向関数として計算され、後に前記チケット供給業者のコンピュータに伝達されたものであり、

数Rは、前記チケット消費者のコンピュータ内にその起源を有し、前記チケット消費者の秘密であり、公でなく、

前記チケット供給業者のコンピュータの前記ディジタル署名鍵sは、前記チケット供給業者の秘密であり、公でない、

ことを特徴とする、印刷チケット担持指標。

【請求項49】　ディジタル・チケットを販売し配信する通信システムであって、

（i）1回目に秘密数の一方向変換を販売者のコンピュータに送り、（ii）3回目に、前記チケット販売者のコンピュータから、署名付き情報を受信し、（iii）4回目に、前記受信した暗号化署名情報を前記秘密数と共に、ディジタル・ストアに格納する、チケットの購入者のコンピュータと、

（i）1回目に、前記販売者のコンピュータからの前記秘密鍵の一方向変換を受信し、（ii）2回目に、この一方向変換および追加情報に署名し、（iii）3回目に、前記署名した第1変換および追加情報を、署名済み情報として、前記チケットの購入者のコンピュータに送る、チケット販売人のコンピュータと、

4回目に、前記署名済み情報および前記秘密数を、ディジタル・チケットとして格納するディジタル・ストアと、

を備え、

（i）前記署名済み情報を読み取るとき、（ii）前記署名済み情報を解読し

売人の安全なコンピュータに双方向通信を行うチケットの購入者のコンピュータを有する通信システムにおいて、チケット販売人からチケットの購入者にディジタル・チケットを販売し配信する方法であって、

1回目として、前記通信ネットワークを通じて、前記チケット販売人のコンピュータから前記チケットの購入者のコンピュータに、チケットを有する目的であるイベントに関する第1データを、第1の送信として送り、次いで、2回目として、

前記通信ネットワークを通じて、前記チケット販売人のコンピュータから、前記チケットの購入者のコンピュータに、チケットを所望するイベントを識別する第2データを、第2の送信として送り、前記第2データには、チケット購入者のみによって決定され、前記チケット販売者を含むその他の者には知られていない数の安全な第1変換を付随させ、

前記通信ネットワークを通じて、前記チケット販売人のコンピュータから、前記チケットの購入者のコンピュータに、前記チケットを所望するイベントに対するチケットの発行を確認する第3データを、第3の送信として送り、該第3データには、前記安全な第1変換の安全な第2変換を付随させ、

前記チケットの購入者のコンピュータを用いて、ディジタル・データ・ストレージの有形可搬媒体内に、（ｉｉ）前記安全な第2変換を伴う（ｉ）前記数を格納し、

（ｉ）前記ディジタル・データ格納媒体の、前記イベントの物理的サイトへの輸送のとき、（ｉｉ）前記購入者が用いたのと同じ安全な第1変換の使用により、前記数をコンピュータに読み込み、前記数の安全な第1変換の再生を再度行うとき、および（ｉｉｉ）前記第2変換を知る特権を有するイベント・コンピュータが前記安全な第2変換を逆転させるとき、（ｉｉ）読み取り再生した第1変換を（ｉｉｉ）前記第2変換を逆に行うことによって再現した第1変換と比較し、前記ディジタル・チケットの有効性判断を可能にする、

方法。

【請求項52】　請求項51記載の方法において、前記第2の送信は、前記数の一方向ハッシュ関数の形態の安全な第1変換を伴う前記第2データについて

【発明の詳細な説明】

【０００１】

（発明の背景）

１．発明の分野

本発明は、一般的に、電子マネー、電子チケット、電子クーポン、電子小切手、ディジタル・チケットなどに関する。

【０００２】

本発明は、特に、（ｉ）安全、迅速、安価そして効率的に生産可能であり、世界中のディジタル通信ネットワークを通じて配信可能であり、（ｉｉ）その購入受信者によって視覚的に検査でき、物理的に安全で輸送可能であり、（ｉｉｉ）捏造に対して強い即ち影響を受けず（しかしながら、ネットワーク侵入者、個々のディジタル・チケットの購入受信者、および／または共謀に荷担する多数の購入受信者が、そのようなディジタル・チケットの捏造を行おうとする可能性はある）、（ｉｖ）購入受信者が望むのであれば、匿名で購入し、保持し、受け戻すことができ、（ｖ）２－Ｄバー・コード・フォーマットのレーザ・スキャニングによる、またはスマート・カードからのデータ読み取りによる等を含む、受け戻し時に容易に、素早く、しかも安全に検証可能であり、（ｖｉ）二重受け戻し、またはあらゆる盗難の報告の後では１回の受け戻しも許さず(resistant)、（ｖｉｉ）移転および分割可能であり、（ｖｉｉｉ）自己認証し、（ｉｘ）様々な資格を組み込む多様性を有し、（ｘ）物理的な弁済(tender)または解約(surrender)なく取り消し可能または受け戻し可能であり、（ｘｉ）生態的に健全な、ディジタル・チケットに関する。

【０００３】

２．従来技術の説明

２．１　一般的な背景

２．１．１　一般的な緒言

会社間および会社－消費者間のトランザクション(transaction)双方における電子商取引(electronic commerce)の量は、近年劇的に増大している。殆どの消費者のインターネット商取引は、クレジット・カードによる処理に基づいており

者によって種々の方法でチケット・イベントの行為地に運ぶことができる。ディジタル・データは、フレキシブル・ディスクに格納したり、スマート・カードに格納したり、紙上に印刷すること等もできる。

【０００７】

本発明の発明者には、印刷した二次元バーコードの使用が、ディジタル・チケット購入のために非常に適したエンコーディング技術として好ましく思われる。ItKin and Josephine Martell; A PDF417 primer: A guide to understanding second generation bar codes and portable data files; Technical Report Monograph 8, Symbol Technologies(１９９２年4月）を参照のこと。また、AIM規格"Uniform Symbology Specification PDF147"も参照のこと。印刷した２－Dバーコードは、収容したデータのフォールト・トレランス性に優れ、再ディジタル化が容易である。このように印刷したディジタル・チケットは、経済的な初期市場浸透が可能であり、チケットの形態およびコンテンツの使い勝手を多少妥協すれば、手元にある消費者のハードウエア基礎構造を利用できる。即ち、多くのウェブ・サーファは、スマート・カード・リーダ／ライタの状況とは異なり、プリンタにアクセスすることができる。

【０００８】

２．１．２　インターネット・チケット発行要件

インターネット・チケットは、アクセス権またはケーパビリティ(capability)のディジタル表現と見なすこともできる。これらは、使用時に消費することができ、あるいはある時間期間にわたって有効とすることができる。例えば、ムービーのチケットと、フィルム・シリーズのシリーズ・チケットの関係である。更に一般的には、このようなチケットは、その使用に制約を設けることができる。例えば、午前講演に5回だけ有効な映画パスがある。

【０００９】

従来のケーパビリティ指向型オペレーティング・システムにおけるケーパビリティとは異なり、ディジタル・チケットのケーパビリティは、チケットの送信や読み取りを行うオペレーティング・システムのカーネルによって維持されない。恐らく、最も近い類似物は、ケーパビリティのAmoeba分散カーネルの使用であり

（４）支払い処理がネットワーク・アクセスを必要とせず、第三者の介入を必要としない、オフライン処理可能性。

（５）電子マネーを顧客間で移転することができる、移転可能性。

（６）交換が容易にできる、分割可能性。

【００１３】

２．１．４　電子スタンプにおけるような情報に基づく証印（ＩＢＩ）

情報に基づく証印は、郵送料を支払ったことを封筒上で示す1つの方法を与える。U. S. Postal Service; Information Based Indicia Program (IBIP) New Technology Metering Devices（１９９５年５月）を参照のこと。ＩＢＩ規格は、この目的のために、ディジタル署名をエンコードした二次元バーコード（ＰＤＦ４１７）を用いている。U. S. Postal Service; Information Based Indicia Program (IBIP) Indicia Specification（１９９６年７月）を参照のこと。また、Stuart Itkin and Josephine Martell; A PDF417 primer: A guide to understanding second generation bar codes and portable data files; Technical Report Monograph 8, Symbol Technologies（１９９２年４月）も参照のこと。

【００１４】

ディジタル郵便料の用途は、インターネット流通ディジタル・チケットに類似しているが、その要件のためにソリューションの複雑化を招いている。ここでは、証印の有効性を判断し、ディジタル署名を検証し、マスタ・データベースと照合して複製を防止しなければならないが、このような複製使用検出は、分散型データベースに頼らざるを得ない場合もある。更に、スタンプの価値が低いことから、場合によっては、非常に安価な詐欺検出対策だけの方が費用効率的であることを暗示している。また、完全にオフラインで印証を印刷し、郵便局における通信の必要性を抑制することができなければならない。このため、郵便セキュリティ・デバイス（ＰＳＤ）が用いられることになる。これは、特殊なセキュア・コプロセッサであり、ＰＳＤが潜在的に敵対的環境にある場合でも、差し引き残高を維持し、暗号計算を実行する安全な方法を提供する。

【００１５】

証印とは異なり、チケットは、通例では、例えば、映画館、コンサート・ホー

トのような用途では一般的であるが、それでも過剰予約の数は制限し管理しなければならない。何故なら、過剰予約は経済的に健全ではないからである。

【００１９】

２．２　具体的な背景

２．２．１　ウェブ・サーバにアクセスするエンド・ユーザに対するセキュリティ

本発明と関連のある従来技術に、カリフォルニア州Mountain ViewのAxent Technologies, Inc. ["Axent"]の、ウェブ・サーバにアクセスするエンド・ユーザのセキュリティを強化するシステムおよび製品がある。この技術が非常に関連深いのは、第1に、サーバが顧客を安全に識別でき、そしてその逆も可能であれば、サーバは顧客にディジタル・チケットを発行することができるからである。

【００２０】

しかしながら、更に重要な比較点は、一層微妙である。本発明は、ある局面(juncture)において、多数のデータ量またはフィールドを暗号化することに着目する。以下の第4パラグラフでは、暗号化量、「メッセージ認証コード」も、Axentシステムにおけるディジタル・チケットの一部であることを明らかにする。

【００２１】

Axent社は、暗号化チケットの生成および流通において、その"Web Defender"サーバ・ソフトウエアは適正な保護を与えるので、ユーザは企業間にまたがる多数のウェブ・サーバにログインすることができ、その都度追加のパスワードを入力する必要はないと言っている。

【００２２】

更に良いことは、Web Defenderは、ネットワーカに、集中的にこれらのチケットを追跡し管理する方法を提供するように要求されるので、個人またはグループの名称で、企業データへのアクセスを制御することができる。設定の間、顧客のブラウザを修正する必要はない。

【００２３】

Web Defenderは、企業のファイヤウオールの背後に潜み、Microsoft Corporation (Redmond, Washington)からのInternet Information Server（ＩＩＳ）を走

２．２．２　以前の特許

Xerox Corporation (Stamford, Connecticut)に譲渡されたStefik, et al.の一連の特許は、ディジタル・チケットを含む（が、これに限定される訳ではない）有価ディジタル・ワーク(work)の頒布および使用を扱う。米国特許第５，７１５，４０３号は、SYSTEM FOR CONTROLLING THE DISTRIBUTION AND USE OF DIGITAL WORKS HAVING ATTACHED USAGE RIGHTS WHERE THE USAGE RIGHTS ARE DEFINED BY A USAGE RIGHTS GRAMMAR（使用権を使用権文法によって規定する場合に、使用権が添付されたディジタル・ワークの頒布および使用を制御するシステム）に付与され、米国特許第５，６３８，４４３号は、a SYSTEM FOR CONTROLLING THE DISTRIBUTION AND USE OF COMPOSITE DIGITAL WORKS（復号ディジタル・ワークの頒布および使用を制御するシステム）に付与され、米国特許第５，６３４，０１２号は、a SYSTEM FOR CONTROLLING THE DISTRIBUTION AND USE OF DIGITAL WORKS HAVING A FEE REPORTING MECHANISM（料金報告機構を有するディジタル・ワークの頒布および使用を制御するシステム）に付与され、そして米国特許第５，６２９，９８０号は、a SYSTEM FOR CONTROLLING THE DISTRIBUTION AND USE OF DIGITAL WORKS（ディジタル・ワークの頒布および使用を制御するシステム）に付与されたものである。最初に本願にも含まれるものとした、"SYSTEM FOR CONTROLLING THE DISTRIBUTION AND USE OF DIGITAL WORKS USING DIGITAL TICKETS"（ディジタル・チケットを用いたディジタル・ワークの頒布および使用を制御するシステム）と題する出願第０８／３４４，７６０号は、まだ特許として発行されていない。

【００２７】

これらの特許は、主に背景として、具体的にはネットワーク上およびこれを通じて通信するシステムのセキュリティの性質に関して、本発明に関連がある。これらの特許における「信頼レポジトリ」(trusted repositories)の使用は、本発明の基本的システムにおける直接的な対抗物の範囲外である。しかしながら、本発明は、全世界的に採用および展開され毎月何十億枚ものチケット発行に使用される可能があり、同じイベントについてでさえも、全てのチケットが同じ発行元から来るとは限らない。したがって、Xeroxの特許は、本発明のディジタル・チ

つ信頼性高く遂行する責任を負うことができるからである。システムが責任を負える（「応答することができる」）ということは、基本的に保全性の問題である。レポジトリの保全性は、３つの部分、物理的保全性、通信保全性、および挙動的保全性を有する。

【００３１】

物理的保全性とは、物理的デバイス自体の保全性のことを言う。物理的保全性は、レポジトリおよび保護対象のディジタル・ワーク双方に適用される。したがって、高いセキュリティ・クラスのレポジトリは、それらの安全ケース上で改竄が行われようとしたときに、検出するセンサをそれら自体が有する場合もある。レポジトリ自体の保護に加えて、レポジトリの設計は、ディジタル・ワークのコンテンツへのアクセスも保護する。フロッピ・ディスク、ＣＤ－ＲＯＭ、およびビデオテープのような、従来の磁気および光デバイスの設計とは対照的に、レポジトリは、信頼のないシステムには、決してワークに直接アクセスさせない。汎用コンピュータ・システムのメーカは、彼らのプラットフォームを用いて不正コピーを作成することはないと保証することはできない。製造業者は、情報を読み取りそして書き込む一般的な機能を提供し、汎用計算機の機能性の総合的な特性はそれに依存する。したがって、コピー・プログラムは任意のデータをコピーすることができる。このコピー問題は、汎用コンピュータに限られる訳ではない。これは、磁気記録装置によるビデオおよびオーディオ記録のような、娯楽用「ソフトウエア」の不正複製についても発生する。この場合も、記録装置の機能性は、そのコピー能力に依存し、コピーが許可されているか否かチェックする手段をこれらは有していない。対照的に、レポジトリは、汎用デバイスによる生データへのアクセスを防止し、コピーやそれ以外のアクセス付与の前に、明示的な権利および条件を検査することができる。信頼レポジトリ間でのみ、プロトコルによって情報にアクセスする。

【００３２】

通信保全性とは、レポジトリ間の通信チャネルの保全性のことを言う。大まかに言えば、通信保全性とは、「うそをつく」ことによってレポジトリを簡単に騙せないことを意味する。この場合の保全性とは、他のデバイスが、認証されたレ

各レポジトリは、特定のセキュリティ・クラスに属するものとして類別される。ある種の通信およびトランザクションは、レポジトリが特定のセキュリティ・クラスに属することを条件とする場合もある。動作の前提条件として、レポジトリは、識別認証書の所有を必要とする。識別認証書を暗号化して改竄を防止し、これをマスタ・レポジトリが発行する。マスタ・レポジトリは、公認エージェントの役割を果たし、レポジトリがディジタル・ワークを受信することを可能にする。識別認証書は、周期的に更新しなければならない。識別認証書については、登録トランザクションに関して、以下で更に詳しく説明する。

【００３６】

レポジトリは、ハードウエアおよび機能的実施形態双方を有する。機能的実施形態とは、通例では、ハードウエア実施形態上で実行するソフトウエアのことである。あるいは、機能的実施形態は、特定用途集積回路（ＡＳＩＣ）チップのようなハードウエア実施形態に具体化することも可能である。

【００３７】

レポジトリのハードウエア実施形態は、安全なハウジング内に密閉されており、危険に晒された場合には、レポジトリをディスエーブルさせることができる。レポジトリのハードウエア実施形態の基本的コンポーネントは、処理手段、記憶システム、クロック、および外部インターフェースを含む。

【００３８】

コア・レポジトリ・サービスは、各レポジトリが必要とする１組の機能から成る。コア・レポジトリ・サービスは、セッション開始トランザクションを含む。この1組のサービスは、ディジタル・チケットを「穿孔する」際に用いる包括的チケット・エージェント、および公認指定(authorization specification)を処理する包括的公認サーバも含む。ディジタル・チケットおよび公認は、ディジタル・ワークの頒布および使用を制御する具体的な機構である。尚、コア・レポジトリ・サービスに結合するのは、複数の識別認証書であることを記しておく。レポジトリの使用を可能にするには、識別認証書が必要となる。

【００３９】

一見使用権について、この方式上における変形(variant)は、ディジタル・チ

トを含む）で作られている場合、新たな所有者は、コピーの販売者がそのワークを使用したか否かには関わらず、未使用の（未穿孔の）チケットが得られることを期待するであろう。対照的に、ワークを貸与したり、あるいは単にそれを他のレポジトリに移転する場合には、チケットを生き返らせるべきではない。

【００４４】

２．２．３　汎用ディジタル・チケットのフレームワーク

NTT Information and Communication Systems LabsのKo FujimuraおよびYoshiaki Nakjimaは、ディジタル・チケットに取り組んでいる。Fujimura氏は、二重使用を防止する包括的価値流通媒体を開発することを主目的とする、柔軟なディジタル・チケットの構想を練っている。このコンテキストでは、チケットは、当該チケットの所有者にある権利を保証するディジタル媒体である。チケットの記述によって、チケットは、単一のチケット（またはそのグループ）において多数の異なる価値や、異なる種類の価値を含むことが一般に可能となる。

【００４５】

Fujimura氏は、汎用チケット・フレームワークは、多くの場合実施コストを低減すると主張する。何故なら、単一の設計を多くの場所で使用することができるからである。一般化することによって、チケットを任意に構成し、バンドリング(bundling)や同様のフィーチャ(feature)を可能とすることができる。彼は、発行／解除サービスや供託ボックス・サービス(deposit box service)のように、このフレームワークを実現する新たなビジネスの創作は有効であったと主張する。

【００４６】

汎用ディジタル・チケット・フレームワークは、ディジタル・キャッシュの要件の殆どを満たさなければならない。追加の要件には次のものがある。（１）チケットは、その匿名性、分割可能性、および移転可能性を、用途に応じて制御することができる。（２）チケットの個々の仕様を「機械理解可能」とし、製品またはサービスの受け戻しを可能にする。（３）流通している間に価値が変化するチケット・プロパティ（例えば、支払いまたは予約ステータス）は、安全に変化させなければならない。（４）１つよりも多いサブチケットから成るチケットに

２．２．４　ＸＭＬチケット：一般化したディジタル・チケット定義言語

日本電信電話（ＮＴＴ）が先頭に立って行動している、「ＸＭＬチケット」と呼ばれる、一般化したディジタル・チケット定義言語を定式化する作業がある。この定義言語、およびこのプロトタイプの規格は、本発明とは全く矛盾しない。この規格は、一般的なフォーマットのディジタル・チケットが何を含むべきかということに関係し、本発明は、どのようにしてディジタル・チケットを安全に生成し、受け戻すかということに関係する。

【００５１】

NTT Information Sharing Platform LaboratoriesのKo Fujimura, Yoshiaki Nakajima, およびJun Sekineは、ワールド・ワイド・ウェブが、日常生活で用いられる様々な種類のディジタル・コンテンツのための情報配信基幹施設を提供すると書いている。ディジタル・キャッシュ、マイクロペイメント(micropayment)、および暗号化クレジット・カードのような支払い基幹施設も確立されている。しかしながら、二重の受け戻しを防止し、種々の権利の取引を可能にする、紙のチケットと同様のディジタル媒体や、基幹施設はまだ確立されていない。

【００５２】

このため、Fujimura、NakajimaおよびSekineの三氏は、あらゆる種類の権利を流通可能な、一般化したディジタル・チケット・システムを開発しようとしている。ディジタル・チケットとは、チケット所有者にある種の権利を保証するディジタル媒体であり、ソフトウエア・ライセンス、リソース・アクセス・チケット、イベント・チケット、航空機チケットなどを含む。共通のチケット処理システムを用いて様々な種類のディジタル・チケットを流通させるために、彼らは汎用ディジタル・チケット・フレームワークの中で、チケット自体に指定されている匿名性、移転可能性、および受け戻し方法のようなチケット・プロパティを、ＸＭＬに基づく一般化チケット定義言語を用いて解釈することによって、チケットを流通させることを提案している。

【００５３】

各用途には、従来のディジタル・チケット・システムが開発されている。しかしながら、Fujimura、NakajimaおよびSekineの三氏は、以下の理由のために一般

スのように、流通中に動的に価値が変化するプロパティの定義に対応しなければならない。尚、これらの変化を署名入り文書で可能にするのは困難であることを記しておく。

【００６０】

（３）機械理解可能性。言語は、チケットの意味の定義付けに対応していなければならない。チケットが保証するサービスまたはタスクが、トランザクションを実行する前に、購入者および販売者によって客観的に理解されれば、チケットの意味の誤解に起因する紛争の数が減少する。

【００６１】

（４）効率。言語は、チケットの効率的な定義付けができなければならない。何故なら、これはスマート・カードまたはメモリが制限された他のデバイスに格納される場合もあるからである。定義が長い程、データ転送時間も長くかかり、したがって受け入れられない可能性もある。例えば、イベント・チケットまたは輸送パスの受け戻しには、高い性能が必要となる。

【００６２】

（５）流通制御可能性。言語は、柔軟な流通制御を可能にするために必要なパラメータを用意しなければならない。表I に示すように、チケットの匿名性、移転可能性、および受け戻し方法は、チケット定義において指定しなければならない。加えて、更に進んだ要件にも対応することが望ましい。例えば、登録したグループのメンバ間でチケットを流通させたり、適格と判断された店舗でのみチケットを発行できるようにする。

【００６３】

（６）セキュリティ。先の研究者は、セキュリティを得るために必要なパラメータを、言語が用意しなければならないことに気が付いた。（本発明は、方法、およびチケットのコンテンツ（その内容を表す言語ではない）が、セキュリティを与えるものであることを教示する。）ディジタル・チケット・システムは、ディジタル・キャッシュ・システムと同様に、二重受け戻しを防止するファシリティ(facility)に対応しなければならない。これには、オンライン通貨チェック・システム、またはスマート・カードのような耐改竄デバイス、およびディジタル

【００６９】

（５）流通制御可能性およびセキュリティ。ＸＭＬはあらゆる構造化データを記述するために設計された包括的言語であり、したがって、チケットの流通を制御するために必要なあらゆるパラメータを定義することができる。これらの要件を満たすために必要な制御パラメータまたはセキュリティ・パラメータを確立することは、チケット処理システムとして、言語に多大な影響を及ぼすことはない。

【００７０】

R. D. Brown, "Digital Signatures for XML", IETF Internet Draft, January 1999; K. Fujimura and Y. Nakajima,"General-purpose Digital Ticket Framework", 3rd USENIX Workshop on Electronic Commerce, August 1998, pp.177-186（ <http://www.usenix.org/publications/library/proceedings/ec98/fujimura.html.>を参照）を参照のこと。また、出版予定のK. Fujimura, Hiroshi Kuno, Masayuki Terada, Kazuo Matsuyama, Yasunao Mizuno and J. Sekine,"Digital Ticket Controlled Digital Ticket Circulation"、Y. Nakajima and K. Fujimura, 未出版の原稿"The XML Ticket Specification"も参照のこと。また、XML Schema Requirements, The World Wide Web Consortium, Note, February 1999（ <http://www.w3.org/TR/NOTE-xml-schema-req>を参照）も参照のこと。

【００７１】

これらの研究の本発明に対する関連性としては、全てが当てはまる。本発明は、ディジタル・チケットを安全に生成し、流通させ、受け戻す態様に関し、ＸＭＬのような進んだ言語でチケット内の情報（更に、チケット流通のパターン、チケットを購入可能な地理的サイトのようなその他の情報）を表現することには異論がなく、実際、同意する点もある。

【００７２】

２．３　ディジタル署名

本発明は、ディジタル署名、暗号化技術における慣例の概念を採用することに着目した。本発明は、ディジタル署名を生成する多くの異なる方式と完全に動作する。

覚えておくことを可能とする。ディジタル・チケットは、（ｉｖ）共通して購入者によってコンパクトな物理形態、最も一般的には印刷した紙片、または、頻度は少ないが、スマート・カードまたはコンピュータ・ディスクのような輸送可能なメモリ・デバイスに還元する。この物理的形態では、ディジタル・チケットは、（ｖ）安全に格納し、ある時点である場所（チケットが最初に配信されたときに決定されている）に輸送し、チケットが購入されたときに決定したある資格、最も一般的にはイベントへの入場のために、受け戻す。受け戻しのために弁済される際、ディジタル・チケットを、（ｖｉ）素早く、安全に、そして費用をかけずに有効性を判断し、検証して、チケットが正当かまたは改竄かについて明確な判断を下す。また、同じチケットまたはそのコピーが1回よりも多く同じイベントのために弁済されているか否か判定を行うこともできる。

【００７６】

１．本発明によるディジタル・チケットの品質

本発明のディジタル・チケットは、費用効率性が高い。即ち、これは、発注、作成、処理、輸送、および弁済が容易であり、能率的であり、費用がかからない。

【００７７】

特に、ディジタル・チケットのこのような部分は、チケット購入者のネットワーク接続コンピュータ内において生成し、計算上集約的でない。このような計算は、通例では、消費者のコンピュータのブラウザ内において走る小型のJava（登録商標）appletによって能率的に実現することができる。（チケット購入者のネットワーク接続コンピュータは、通常更に強力であるが、必ずしもそうとは限らない。）ディジタル・チケットの購入も、伝送も、大量の情報のネットワーク通信を全く伴わない。したがって、ディジタル・チケットの購入は、通常、電子商取引の処理と同じくらい速いか、またはこれよりも速く終結する。

【００７８】

ディジタル・チケットの購入は、あらゆる電子商取引の処理と同じ位容易である。購入者は、当該注文について、パスワードも、コードも、キーも何も考えさせられず、覚えておく必要もない。

ディジタル・チケットは製作において安全である。正当なチケットの暗号によって保護された部分は、安全な設備において、チケット製作者および販売者によってのみ作成することができる。更に、チケットの購入者の手にあるディジタル・チケットのセキュリティは、いずれの物理的デバイスにも依存せず、暗号に依存する。有効なディジタル・チケットを詐欺的に作成することは、実際には不可能なレベルにまで困難である。チケット消費者／購入者およびチケット提供者／販売者間の二方向の各々において伝達される情報は暗号化されているが、ディジタル・チケットのセキュリティは、暗号分析的セキュリティに基づくだけでなく、署名鍵と呼ばれる、鍵の物理的セキュリティにも基づいており、これはチケット製作者／販売者にしか知られていない。

【００８３】

ディジタル・チケットは、受け戻しにおいて安全である。正当なディジタル・チケットの不正な複製も場合によっては可能な場合もあるが、単純な１回だけ最初に提示されたディジタル・チケットでさえも、チケットの動作によって予約されたいずれか１つの開催またはイベントについては受け戻される。有効なディジタル・チケットのコピーを作ることは、本質的に無価値である。

【００８４】

ディジタル・チケットのセキュリティは見ることができる。改竄または不正なディジタル・チケットは容易に検出され、最も好ましくは、コンピュータが駆動するディスプレイによって、弁済された不正チケット上で、不正な２－Ｄバーコードを、正当であればその特定のチケットが所有するはずの正当な２－Ｄバーコードの近くで、表示することによって検出することを含む。このような視覚表示は、門番およびチケットを弁済しようとする人双方に、何故チケットが不正と見なされるのかについて的確な視覚表示を与える。

【００８５】

本発明のディジタル・チケットの購入および受け戻しは、チケット購入者／消費者およびチケット製作者／販売者間、ならびにチケット受け戻し人およびチケット集札人間（受け戻し人および集札人のいずれかまたは双方は、チケット購入者／消費者またはチケット製作者／販売者と同じ人である場合も、ない場合もあ

受け戻しと相関付けることもできる。本発明のディジタル・チケットは、通常保持者同士でしかるべきときに容易に移転および再移転が可能であることから、分割の対象となるチケット内にあるあらゆる権利は、分割することができる。例えば、チケットが、日付を指定しない午前中のフィルムに5回だけ有効である場合、5人の異なる人が、各々、午前中に同じ時刻または異なる時刻にチケットを1回だけ用いることができる。（多数のイベントに対するチケットの受け戻しは、未使用の多数使用チケットおよびチケットの部分的受け戻しを記憶した、ネットワーク状コンピュータによって行われる。）

（本発明の下では、チケット購入者／チケット受け戻し人の匿名性を保存できるという概念とは逆に、コンピュータを用いて、チケット発行およびチケット受け戻しプロセスの絶対的にあらゆる面をリアル・タイムで監視し制御することも、代わりに可能である。したがって、"Doctor Jones"のコンピュータ上に残っているデータにアクセスした者は、ゲームの時間にフットボール・スタジアムに電話をかけ、「Dr. Jonesはゲート E 3 に2：２２ＰＭに入り、指定座席が４３Ｌ２２である」ことを告げられるということも可能である。）

本発明のディジタル・チケットは、キャンセル可能であり、したがって、物理的にディジタル・チケットを再所有することなく、代金全額を払い戻すことができる。

【００８９】

本発明のディジタル・チケットは、柔軟性があり、多様性がある。いずれの1枚のチケットでも、あらゆる所望の資格の組み合わせに合わせることができ、いずれの1つのイベントにチケットを提示しても（または提示しなくても）、別のイベントのために後にそれを提示する際には影響はない。購入したチケットを印刷した紙が薄く、使用のために磨耗した場合、または磨耗すると予想される場合、多数のコピーを印刷してもよい（しかし、同時に詐欺的に受け戻してはいけない。上記参照）。

【００９０】

単一使用チケットは、通常、収集されず、価値を損なうこともなく、イベントにおいて物理的に破損することもなく、潜在的にチケットの紙屑となる。実際に

普通に購入する。通信ネットワークへの接続、特にインターネットへの接続は、事実上チケットを得る唯一の実用的方法となる。

【００９５】

第2に、チケットは、チケットの購入者あるいは彼または彼女の代理人によって、印刷するか、可搬性メモリ媒体上に格納するか、またはスマート・カード上に格納しなければならない。それぞれ、チケット購入者は、コンピュータ・プリンタ、ディスク・ドライブ等、またはスマート・カード・ライタを所有していなければならない。

【００９６】

第3に、チケットが与える資格が大量の貨幣価値があり得ることには無関係に、ディジタル・チケットは購入者が印刷するので、地味な外観に過ぎず、色も白黒であると思われる。これは、単に、ディジタル・チケットは、それが具体化する権利と同じように高価には見えない場合もあるということを意味するに過ぎない。

【００９７】

第4に、チケット検証、チケット受け戻し、およびゲートでの監視における最高度の品質および処理能力には、（ｉ）コンピュータ、好ましくは、ネットワーク・コンピュータ、および（ｉｉ）ディジタル・チケット・リーダ、最も一般的には、光学式リーダが必要となる。チケットに関係するイベントの場所またはその近くで、通常、電力が必要となる。チケット検証および受け戻しプロセスにおいては、単一のコンピュータもリーダも連続する信頼性エレメント(serial reliability element)とはならないが、さんざん待たされたイベントへの迅速な入場処理を待っている大観衆のために、フェール・セーフの要件が生ずる場合もある。使用する（ｉ）コンピュータおよび（ｉｉ）リーダ・ハードウエアは、通常信頼性があり、および／または冗長であり、ディジタル・チケットの処理が停滞したり遅れたりすることを未然に防ぐ。（尚、イベントへの予想入場者の大半は正当なチケットを有するが、携帯プリンタを手にしていないこと、および電子入場システムが故障した場合、弁済されたチケットを、イベントの入場口でソートした、予め印刷してあるチケットの台帳と比較したり、あるいは単にチケットを示

【０１００】

数Ｒは、オプションとして追加的に、例えば、（ｉｉ）消費者のアイデンティティ、（ｉｉｉ）チケットを求めたイベント、および入場者数、および／または（ｉｖ）支払いが必要な場合、チケットに対する支払いの基準というような他の情報を含むこと、またはこれらを伴うこともできる。注意すべきは、これらの情報（ｉｉ）－（ｉｖ）のいずれも、数Ｒに組み込む必要はなく、数Ｒは、（ｉ）乱数成分のみを含んでいればよい。数Ｒ内（そして、究極的に、消費者に提供するディジタル・チケット内）への消費者の名前の加入のような、彼／彼女の情報の提示も完全にオプションであることが容認できることが好ましく、消費者がこの情報を提供することに同意しない場合、ディジタル・チケット発行プロセスには引き続き障害がなく、実質的に等質である。

【０１０１】

次に、チケット消費者のコンピュータは、数Ｒの一方向関数、即ち、hash(R)つまりh(R)を計算する。この一方向関数は、元の数Ｒをhash(R)から導出することができるように計算上逆算しにくく、数学的に認められている多くの異なる関数のいずれでもよい。ＳＨＡ１およびＭＤ５関数は特に適しており、好ましい。hash(R)は、２ステップ除去した先行物、即ち、「第2先行物」と見なすことができ、最終的にディジタル・チケットとなる。

【０１０２】

次に、この計算したhash(R)を、チケット消費者のコンピュータからチケット供給業者のコンピュータに、通信チャネルを通じて再度送信する。情報（ｉｉ）－（ｉｖ）のいずれかのような、追加のチケット発注データが、hash(R)の第2送信に伴うことができ、一般にはそうしている。全ての第2送信は、チケット販売者のコンピュータ、通常はインターネット上のサーバと、ブラウザ・プログラムを走らせているチケット消費者のクライアント・コンピュータとの間に確立されているような、安全なチャネル（ＳＳＬ、即ち、セキュア・ソケット・レベル）上で送ることも可能である。しかしながら、本発明の方法では、hash(R)を送信することのみが必須である。例えば、セット・イベントのためのチケットを、自由に先着順で全ての来訪者に頒布することが想像できる。この場合、実際に追

この数Sign(s,I||hash(R))||Rは、通常、所定サイズの二次元バーコードとして編成され、表示される。ＰＤＦ４１７およびＱＲ二次元バーコード規格が好ましい。

【０１０７】

チケット消費者のコンピュータは、受信した情報（即ち、Sign(s,I||hash(R))）および格納してある情報（即ち、Ｒ）双方からディジタル・チケットを計算し、次いでこの完成したディジタル・チケットSign(s,I||hash(R))||Rを輸送可能な記憶媒体に書き込む。

【０１０８】

この記憶媒体は、消費者のコンピュータが輸送、および内部に格納してあるディジタル・チケットを検索するようにインターフェースに適しているのであれば、それ自体のメモリとしてもよい。この記憶媒体は、消費者が所有しているのであれば、スマート・カード、または磁気ディスク、またはＣＤ／ＲＯＭのメモリとしてもよい。現在（２０００年頃）では、これらのデバイスおよびその媒体は、ディジタル・チケットを格納するのに必要または望ましいものよりも高価であり、入手しずらく、有する記憶容量がはるかに大きい。

【０１０９】

記憶媒体は、普通の紙として、消費者のコンピュータによって印刷することが好ましい。紙のチケットは、（ｉ）二次元バーコード、およびオプションとして（ｉｉ）チケット供給業者、および／またはチケット消費者自身のいずれかがオプションとして提供することができるような、一人の消費者に特定のあらゆる情報、更に（ｉｉｉ）オプションとして提供できるような、イベントおよび特定のチケットに関するあらゆる包括的情報を示す。例えば、チケット消費者が彼／彼女の名前を提示した場合、紙のチケットには（ｉｉ）この名前を印刷することができる。通常ではチケットの使用のために、チケット保持者のアイデンティティの確認が必要であるが、以下で論ずるように、チケット上に名前があれば、例えば、（ｉ）チケットを適用するイベントが些細なことを除外する場合、および／または（ｉｉ）いずれかの個人またはグループが不正な収用、複製または彼／彼女／彼らのチケットを主張している場合、有用であるとすることができる。更に

))||Rを読み取ったなら、Ｒを抽出し、後に用いる。次いで、ディジタル検証鍵ｖを用いてSign(s,I||hash(R))を解読し、I||hash(R)を取得する（これは、思い出されようが、全く関数ではなく、単にI およびhash(R)の組み合わせに過ぎない。）。次に、抽出したＲを用いて、消費者のコンピュータが以前に用いていたのと同じ一方向関数を用いて、新たなhash(R)を新たに計算する。解読したhash(R)を新たに（再）計算したhash(R)と比較する。

【０１１２】

読み取ったSign(s,I||hash(R))||Rが、（１）Sign(s,I||hash(R))部分において、ディジタル検証鍵ｖの使用によって解読されてI||hash(R)が得られ、かつ（ｉｉ）解読したhash(R)が新たに（再）計算したhash(R)に等しい場合、ディジタル・チケットは本物である。これら２つの条件のいずれかが欠ける場合、ディジタル・チケットは捏造である。即ち、（ｉ）解読または（２）比較に失敗した場合、チケットは無効となる。

【０１１３】

双方の条件を満たす場合、即ち、ディジタル検証鍵ｖを用いてI||hash(R)を得る解読が行われ、新たに（再）計算したhash(R)が、その生産およびこの特定の選択したイベントのための配信時にディジタル・チケット内に元々格納されているのと同じ量に等しい場合、チケットは適正なイベント（Ｉによって定義される）のためのものに違いなく、特定のチケットが最初にこのように提示されたのか否か、更に評価しなければならない。読み取った（そして解読した）ディジタル・チケットのコンテンツが最初に一意に提示された場合、ディジタル・チケットの保持者はイベントへの入場が許可される。逆に、読み取ったディジタル・チケットが最初にそのように一意に提示されたのではない場合、ディジタル・チケットの保持者は、通常入場を拒否される。

３．　ディジタル・チケット配信システム

本発明の態様の別の１つにおいて、通信ネットワークを通じてディジタル・チケットを配信するシステムに本発明を具体化する。この態様では、本システムの機能性をどのように区分するか検討するとよいであろう。チケット消費者およびチケット供給業者のコンピュータの各々において正確に何が行われるのか、そし

【０１１７】

４．　ディジタル・チケット

本発明の態様の更に別の１つでは、チケット消費者が通信ネットワーク上で、チケット供給業者との双方向処理によって調達したディジタル・チケットに、本発明を具体化する。本発明のこの態様において、ディジタル・チケット内に正確に何があるか、適正かつ正確に、情報操作および交換のどのシーケンスがこれらのコンテンツに繋がるのかについて専念する。

【０１１８】

ディジタル・チケットは、Sign(s,I||hash(R))||Rを含む有形輸送可能データ記憶媒体内に具体化され、（ｉ）Ｒは、チケット消費者の秘密の乱数であり、（ｉｉ）hash(R)はＲの一方向関数である数であり、（ｉｉｉ）I||hash(R)は、チケットが有するイベント（または権利）に関する情報Iの、hash(R)との添付即ち組み合わせであり、（ｉｖ）Sign(s,I||hash(R))は、チケット供給業者の秘密の署名鍵s とI||hash(R)との組み合わせをディジタル署名し暗号化したものであり、（ｖ）Sign(s,I||hash(R))||Rはこのディジタル署名暗号にＲを添付したものである。

【０１１９】

更に詳細には、ディジタル・チケット内にあるこれら数学的量の各々の起源は、（ｉ）チケット供給業者のコンピュータ、または（ｉｉ）チケット製作者のコンピュータのいずれかに記述してもよい。チケット消費者が通信ネットワーク上でチケット供給業者との双方向処理によって調達したディジタル・チケットは、常に、Sign(s,I||hash(R))||Rを含む有形輸送可能データ記憶媒体内に具体化される。しかしながら、詳しくは、この数がどのようにしてディジタル・チケット内に収まるかというシーケンスは、いくつかのステップから成る。

【０１２０】

最初に、Ｒは、チケット消費者のコンピュータにおけるその起源を有する数である。

第2に、Ｒの一方向関数、即ちＲについて計算したハッシュ、あるいはhash(R)は、その起源をチケット消費者のコンピュータ内に有する。

ンピュータは、それが乱数を有する場合にのみ、この一方向ハッシュ関数を生成することができるが、初期状態ではこの数を有していない。

【０１２６】

チケット製作者のコンピュータは、ネットワークを通じて、生成元である消費者のコンピュータから、一方向ハッシュ関数を受信し、消費者のコンピュータが生成することができない何か、署名付きディジタル署名を生成する処理に進む。消費者のコンピュータは、製作者のコンピュータの秘密署名鍵を有していれば、この署名手順をそれ自体でも行うことができるが、有していない。

【０１２７】

直ちにわかるのは、ディジタル・チケットに関係するネットワーク上の通信トラフィックの一部または全部を傍受する者でも、（ｉ）チケット消費者のコンピュータの乱数（前述の章におけるＲ）、または（ｉｉ）チケット製作者のコンピュータの署名鍵（前述の章におけるｓ）のいずれも判断できないということである。

【０１２８】

消費者のコンピュータは、製作者のコンピュータから、ネットワークを通じて、それ自体の（以前に送信した）一方向ハッシュ関数に今では署名されたものを受信し、単に元の乱数を添付し、複合体をディジタル・チケットとして格納する。

【０１２９】

最初にチケットを受け戻すときに、製作者のコンピュータ、またはより可能性が高い門番のコンピュータは、少なくとも製作者のコンピュータのディジタル署名をどのようにして解読するかに関して、製作者のコンピュータと内密関係にあり、直ちに、最初に、乱数にアクセスすることができる。この数はクリア・テキストである。この乱数を取り出し、門番のコンピュータは、次に、チケット製作者のコンピュータの暗号化署名に対するそのディジタル検証鍵（前述の章におけるｖ）の知識を用いて、一方向ハッシュ関数を再現する。

【０１３０】

チケットが正当であった場合、署名データの解読に成功している。門番のコン

関数である必要はなく、一例として、これ自体も暗号とすることもできる。暗号は、結局、究極的なハッシングの形態と見なすことができる。

【０１３５】

次に、本発明、および本発明に関するこの明細書の特許請求の範囲は、前述のように、本発明の理念が単に好適な実施態様の戦略よりも広いことが一旦わかったなら、どのように理解すべきか。前述の第1 および第4 章を理解した上で、本発明の性質について考え、理解する更に別の方法は、最終的なディジタル・チケット Sign(s,I||hash(R))||Rについて検討し、このディジタル・チケットを分解して、タマネギのようにその層をはがして行き、ディジタル・チケットが正確に何で構成されているかを言葉で（同様に数学で）表すことであろう。

【０１３６】

最初に言えることは、ディジタル・チケットは、クリア・テキストになっている何か、乱数を含むということである（または、本発明の何らかの変形では、暗号化されている場合、提示者の暗号鍵を適用することによって直ちにクリア・テキストに戻すことができる）。この何か、このRは、チケット消費者が作成した。しかしながら、最も典型的には、このクリア・テキスト量Rが最初に最終的にチケット供給業者に知られるまでには、通常長い時間が経過し、通常では、チケットを保持する目的のイベントにおいて、ディジタル・チケットの提示時でなければ、知られない。チケット消費者は、したがって、一方向関数hash(R)の使用によって、この乱数をチケット販売者から、そして世界中から隠蔽する。

【０１３７】

次に、ディジタル・チケットも何かを含む。即ち、少なくともチケットを保持する目的のイベントに関する情報I であり、この情報I は、推測されることがあり、安全ではない。ディジタル・チケットのセキュリティは、Sign(s,I||hash(R))||Rにおける、秘密署名鍵s を用いた、hash(R)およびI 双方のディジタル署名にある。この量は一般に通例では公開の鍵v を用いて誰にでも平文に解読することができるが、秘密鍵である署名鍵の知識がなければ、これを行うことはできない。したがって、チケット販売者のみが、ディジタル・チケット自体の最終的な先行物を作ることができる。

し、これによってチケット販売者は、相対的にのみ、チケットの購入者を、多くのチケット購入者から、名前による等して、絶対的ではなく特定することができる。この第1種データは、通常、しかしながら、チケット販売者が特定のイベントおよびチケットの時刻を絶対的に識別することを可能にする。

【０１４２】

更に重要なことは、媒体は、ディジタル署名された量を含む第2種データも有することである。これは、元々次のシーケンスでコンピュータによって発生するものである。（ｉ）１回目に、チケットの購入者によって第1に「１回目に作られた不可逆関数」と呼ばれる乱数の不可逆関数として発生し、次に（ｉｉ）２回目に、チケットの販売人によって、第1に作られた不可逆関数のディジタル署名として発生し、次いで（ｉｉｉ）３回目に、第3に、全く同一の乱数を添付するチケットの購入者によって発生する。ここでは、連続ステップ（ｉ）－（ｉｉｉ）に含まれるものは、本発明のディジタル・チケットに必須である。

【０１４３】

このように構成したディジタル・チケットは、チケットの受け戻しを行おうとするときに、段階を踏んでその有効性を判断する。最初に、乱数を取り出す。次に、署名されている、１回目に作られた不可逆関数を解読し、１回目に作られた不可逆関数を再現する。次に、この取り出された同一乱数の不可逆関数を、再度作る。この新たに作った不可逆関数を、「２回目に作られた不可逆関数」と呼ぶ。

【０１４４】

（ｉ）２回目に作られた不可逆関数が、１回目に作られた不可逆関数に等しく、（ｉｉ）「署名したデータ」の検証および解読に成功した場合、チケットは有効である。２回目に作られた不可逆関数が1回目に作られた不可逆関数に等しくない場合、またはチケットのディジタル署名を検証することができない場合、チケットは、少なくとも特定のイベントについては、無効となる。

【０１４５】

本発明のこれらおよびその他の態様および属性は、以下の図面および添付した明細書を参照することによって、ますます明確となろう。

と呼ぶこともある。

【０１４９】

奇妙なことに、そして慣例では、第1の当事者をディジタル・チケットの「発生者」とも呼ぶことがあるが、ディジタル・チケットを印刷する、あるいは印刷または格納によって有形媒体にそれを変換するのは第2の当事者である。

【０１５０】

この明細書において、各当事者を呼ぶ異なる用語の全てをワープロで処理し、1つ、またはせいぜい2つの異なる用語または記述を各当事者毎に当てることは単純なことであろう。しかしながら、そうすると、ある当事者が活動しているコンテキスト、および本発明の微妙さ双方の理解を阻害することがわかった。したがって、多数の代わりの名前を保存してある。

【０１５１】

２．紙を用いたディジタル・チケット

本発明は、かなりの既存のインターネット技術に影響を与え、使用が容易なソリューションを得た。

【０１５２】

第1に、消費者はＳＳＬ機能付きブラウザにアクセスし、信頼して、暗号化および認証接続を、商人／チケット発行サーバに対して確立する。加えて、図1に示すディジタル・チケット１の好適な第1の印刷による実施形態では、消費者ユーザがプリンタにアクセスできることを想定している。（同様に、図2に示すディジタル・チケット２の第2の可撓性ディスクの実施形態では、消費者ユーザは、磁気可撓性ディスク・ドライブを有していなければならず、図3に示すディジタル・チケット３の第3のＣＤ－ＲＯＭの実施形態では、消費者ユーザは書き込み可能なＣＤ－ＲＯＭドライブを有していなければならない。）

消費者は、彼／彼女のブラウザを用いて、チケット発行サービスのウェブ・サーバに接続し、クレジット・カードのトランザクションのような、標準的な支払い機構を用いて、チケットを購入する。チケット発行サーバは、最も好ましくは、２－Ｄバーコードの形態（そして、オプションとして、何らかの添付テキスト）に編成して、チケットを消費者のブラウザに配信する。次いで、図1に示すデ

ットが保証する資格までに残された時間双方を大幅に、通例では何倍も超過するため、この選択肢は現実的でない。

【０１５６】

加えて、そして更に、hash(・)は衝突に耐えるハッシュ関数であることが好ましく、数R_1のhash(R_1)は、R_1が数R_2から非常に接近しており、たとえ1だけ離れていても、数R_2のhash(R_2)には接近していないことを意味する。数学的関数SHA1およびＭＤ５は特に適しており、好ましい。この好ましい衝突抵抗性の有効性、この有効性は、チケット販売者による二重受け戻しの虚偽請求に関するが、以下で論ずる。しかしながら、目下のところ、ディジタル・チケットのセキュリティはhash(R)関数を逆算することの計算上の困難さにあると早まって推測してはならない。実際、このハッシュ関数は、最終的なディジタル・チケットの高潔さを、どう見ても正直と思われるディジタル・チケットの販売者によるあらゆる不正な操作から保護するためにのみ作用する。

【０１５７】

（３）チケット・サーバ／販売者は、（ｉ）ある情報を添付し、（ｉｉ）ディジタル署名鍵s を用いて、受信したhash(R)および添付した情報I に署名してSign(s,I||hash(R))とし、（ｉｉｉ）この署名したデータ量を、同じディジタル通信ネットワーク５を通じて消費者に返送する。（ここで、x は、チケット・サーバ／販売者からの適切な解読アルゴリズムおよび／または鍵の知識を有する者によって、署名Sign(x)から再現できると仮定する。検証鍵v 、そして時として署名鍵s に対応するアルゴリズムも、通常は公である。しかしながら、チケット消費者／ユーザもチケット販売者以外の何人も、ディジタル的に署名された量Sign(s,I||hash(R))を生成する手段を有していない。）

（４）消費者／ユーザは、しかしながら、何かを暗号化量に追加または添付することができ、この消費者／ユーザは、hash(R)の基本であった同じＲを添付する。（チケット・サーバ／販売者にはこのＲが決して通知されず、そうしたくても、それを返送できないことを思い出されたい。）量Sign(s,I||hash(R))||Rは、論理的なディジタル・チケットとなる。

【０１５８】

り返され、更に好ましくは、図示のように二次元バーコード１１である。印刷した二次元バーコードは、ＰＤＦ４１７またはＱＲ規格によれば、更に一層好ましい。

【０１６３】

この方式の制約は、ディジタル・チケット１が紙上でゲートに輸送されるという要件のために、受け戻しプロトコルを単一のメッセージで構成しなければならないということである。あらゆる検証情報（本発明のＲのような）は単一ステップで解明されるので、チケットをスキャンする者が、チケットが前に受け戻されたと虚偽の主張を行うことを防止するものは何もない。（このような虚偽の主張は、チケット販売者またはチケット受け戻し人のいずれによる不正行為を必ずしも示す訳ではない。従業員の門番が、彼の友人を不正に入場させ、盗まれた座席の正当な保持者を追い返そうとしている場合もある。）しかしながら、チケットをスマート・カードに格納すれば、双方向処理プロトコルの実現が可能である。双方向処理の使用には、次の利点がある。チケットをスキャンする者が、このような早期のチケット受け戻しの虚偽請求を行うことを防止することができる。これについて次に調べる。

【０１６４】

２．１　ディスクおよびスマート・カードを用いたディジタル・チケット

図1に示した本発明のディジタル・チケット１の印刷による実施形態に保持されるのと同じ情報、そしてそれ以上の情報が、図2に示す可撓性ディスク２のような実施形態の中に容易に保持することができる。この可撓性ディスク２は、ＣＤ－ＲＯＭ、ＤＶＤ、およびスマート・カード（図示せず）を含む、多数の他の種類の輸送可能な磁気および光学格納媒体と、サイズ、体積および面積がほぼ一致することは理解されよう。とは言え、これら周知の物理的形態は、図２の可撓性ディスク２のように、個々に図示されていない。何故なら、このような図は本発明の理解には全く何も追加しないからである。機能的観点から最も興味深い形態は、スマート・カード（図示せず）である。

【０１６５】

スマート・カードをディジタル・チケット・コンテナとして用いることにより

トまたは資格に用いられる場合、再び取り上げなければならない。）

ハッシュ関数は衝突に強い（そして、第2予備画像に強い）ので、チケットをスキャンする者（またはチケット発行者）は、二重受け戻しのために顧客を陥れることはできない。スキャンする者の挑戦集合Ｃの委託は、スマート・カードに、それがチケット受け戻しプロトコルの中にあったことを示させ、プロトコルがどういうわけか中断された場合、それが離れたところから継続する。

【０１７２】

２．　関連システム

インターネット補助チケット発行に関連するいくつかのシステム、およびクーポンの発生のような関連する使用がある。これらのシステムについて、この第2章で論じ、本発明の方式と比較する。

２．１　共有認証コード

チケット発行に類似したサービスを提供する方法がいくつかある。最も簡単な方法の1つは、インターネット上および電話のトランザクションのために既に採用されているが、秘密認証コードを「予約番号」として用いることである。これらの秘密コードを記憶するか、書き留めておき、通例では、商用データベースにおいて予約エントリを一意に識別するためにのみ供する。顧客が到着すると、元のクレジット・カードおよび写真ＩＤが要求され、ホテルにチェック・インするかまたは物理的チケットを受け取る。勿論、消費者がコードをキー・インして自動ゲートを操作する場合に、これらのコードの使用を想像することもできよう。

【０１７３】

このようなコードは、ネットワークで配信可能であるが、用いるのが難しい。大観衆がいる行為地へのチケットでは、コードが長くないと、有効な全てのコードの端数が受け入れられない程大量となる。そして、コードが長いと、ユーザはそれを暗記したり、適正にキー・インすることに困難を感じる。

【０１７４】

２．２　ＥＴＭ

既存のチケット発行システム（２０００年頃）にＥＴＭがある（<http://www.etm.com/>）。ＥＴＭはキオスクを基盤とする。消費者は、通例では食料品店内

およびLiberty Production, "<http://www.autoshowusa.com/>において使用可能なクーポンを頒布しており、例えば、彼らのウェブサイトからInternational Auto Showに用いることができるクーポンを頒布している。

【０１７８】

ウェブ・ページ上の指示にしたがって、ユーザは、画面上にクーポンを表示させ、このクーポンを印刷する。その結果、ユーザは、印刷したクーポンを持って行き、店舗またはイベント・サイトにおいて何らかの割引特典を受ける。クーポンは一種の販売促進戦略であり、したがって、捏造に対して特に検討することはない。

【０１７９】

２．５　電子小切手

電子小切手は、単一使用権をエンコードするという点で、チケットやクーポンと同様である。B. Clifford Neuman and Gennady Medvinsky; Requirements for network payment: The netcheque perspective; in Proceedings of IEEE COMPCON'95, March 1995を参照のこと。ここでは、ケーパビリティは、チェック・ライタのチェック口座から受領人自身の口座にマネーを移転する権利である。物理的なチェックには、広範な決済基幹施設があるので、NeumanおよびMedvinskyはこの基幹施設を用いて電子小切手の決済において役立てようと提案した。このような決済基幹施設は、電子チケットには使用できないし、必要性もない。

【０１８０】

２．６　チケット・データ

Fujimura およびNakajimaは、電子チケットおよびクーポンのデータ・エンコーディング要件を検査した。彼らは、ＸＭＬを用いてデータをエンコードすることを提案し、提示すべきチケット・プロパティのリストを与えた。この研究は、本発明に直交し、２つは組み合わせて用いることができる。この明細書の発明の背景の章を参照のこと。

【０１８１】

３．　互換性のあるハッシュ関数

本発明の有効性もセキュリティも、乱数の選択や、チケットの購入者のコンピ

、署名者は最初に、長さk_0のランダム・シードrを選択する。ここで$k_0<k$は方式のパラメータである（$k=|N|$であることを思い出されたい）。次に、特定的な方法であるハッシングを用い、署名者はMおよびr から画像点$y=Hash_{PSS}(r, M) \in Z_N^*$を生成する。すると、通常と同様、署名は$x=f^{-1}(y)=y^d \mod N$となる。検証は更に困難である。何故なら、Mの確率的ハッシュを単純に再計算することができず、同じ値を得ることを期待できないからである。それでも、検証は、１回のＲＳＡ暗号化および何らかのハッシングのみで済む。

【０１８５】

この別の出願の方式は、ＲＳＡに基づく公知の署名方式と同じ位効率的であると主張している。更に、前述のように、関連出願のハッシング方式は、ＲＳＡアルゴリズム自体のセキュリティに緊密に関係することも主張している。したがって、例えば、ＲＳＡ逆転確率が元々2^{-61}であった場合（ある量の計算リソースを用いる）、署名方式に対する捏造の確率は、殆ど等しく低くなる（同じ計算リソースを仮定する）。

【０１８６】

この別の関連出願によれば、「メッセージ再現」を伴う署名も提供する。この技法は、署名したメッセージを送るために必要な帯域幅を減少させる。この技法では、メッセージMおよびその署名x を送信するのではなく、長さが$|M|+|x|$未満の単一の改良した署名τを送信する。検証部は、τからMを再現し、同時に信憑性をチェックする。セキュリティ・パラメータ$k=1024$の場合、この発明方式は、合計k ビットのみを送信することによって、例えば$n=767$ビットまでのメッセージを認証することができると主張する。メッセージ再現を伴う署名方式は、これを達成する際に、メッセージを適切に署名に折り込み、検証部がそれを再現できるようにした。計算上の効率およびセキュリティは、最初に説明した方式と同じである。

【０１８７】

このように、この別の出願の態様の１つでは、データ・ストリングに署名する方法に関する。この方法は、段階的に進み、（ａ）データ・ストリングおよびシ

ングおよび署名技法について述べたのは、主に、本発明が暗号の非常に強力で最も進んだ現在の最前線に完全に結びつくことができるという一例としてに過ぎない。暗号技術の実践者には、本発明は安価な紙の小さな印刷領域に具体化することができるが、このように提示された情報の精巧性およびセキュリティは非常に大きいことが理解されよう。本発明のシステムおよび方法の実世界における使用において常に呼び起こされるセキュリティのレベル、暗号分析的セキュリティおよびその他は、２０００年頃では、恐らく１００米国ドル程度の単一チケットの価値を適切に保護するだけでなく、あるイベントに対して販売されるチケット全ての価値を保護するものであり、主要なスポーツ・イベントであれば、何千万米国ドルとなり得ることも希ではない。

【０１９１】

この他の出願の内容は、この言及によって、本願にも含まれるものとし、それに対するアクセスが、本願に対するあらゆる特許の発行、またはその他のあらゆる状況に必要となる程に、このようなアクセスが本願および別の出願双方の共通譲受人である、Regents of the University of Californiaによって付与される。

【０１９２】

４．　結論

本発明によれば、インターネット上でチケットを購入し配信することができる方式を教示した。発明者は、これらの方式は実用的であり、セキュリティ、消費者アクセス可能性、および使いやすさの間で適度のバランスが得られると確認する。例えば、本発明によるディジタル・チケットは、図4の従来技術の表1に纏めた様々なチケットの種類全ての要件全てを満たす。表1は、<http://www.w3.org/Dsig/signed-XML99/pp/NTT#xml#ticket.html>においてワールド・ワイド・ウェブ上に（２０００年頃）出現したK. Fuhimura, Y.NakajimaおよびJ. Sekineによる論文"XML Ticket; Generalized Ticket Definition Language"から採用したものである。

【０１９３】

前述の説明によれば、本発明によるディジタル・チケット、およびディジタル

【図２】

図２は、本発明によるディジタル・チケットの第２の可撓性ディスクの実施形態を示す図である。

【図３】

図３は、本発明によるディジタル・チケットの第３のＣＤ－ＲＯＭの実施形態を示す図である。

【図４】

図４は、具体的な種類のチケット例のプロパティを示す従来技術の表１であり、その全ては、既に図１ないし図３に示した、本発明によるディジタル・チケットによって実現するのに適したものである。

【図５】

図５は、ディジタル・チケットを配信するための本発明によるプロトコルの概要を説明するテーブル、および付随する通信ネットの模式図である。

【図６】

図６は、ディジタル・チケットを検査するための本発明によるプロトコルの概要を説明する表である。

【 図２ 】

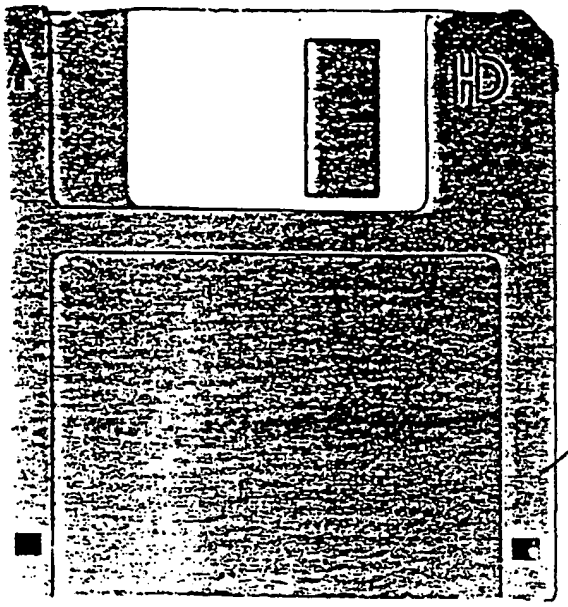


Figure 2

【 図３ 】

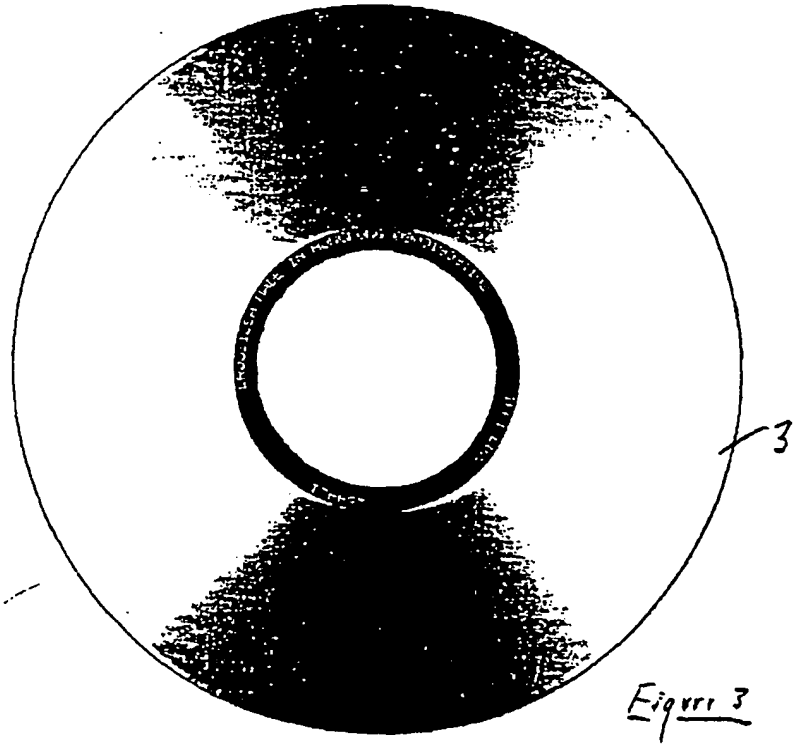


Figure 3

チケット配信プロトコル

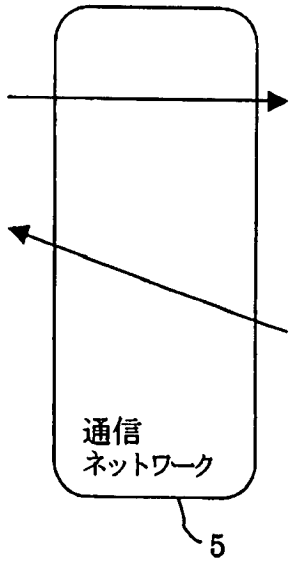
■購入者（ブラウザ）

－乱数Ｒ作成

－hash(R)送信

－チケット受信およびＲ添付
(I||hash(R))s||R

－２Ｄバー・コード画像に印刷または
スマートカードに格納



■プロモータ（サーバ）

－イベント情報Ｉ作成

－hash(R)受信

－ディジタル署名(I||hash(R))s を
用いてチケット作成

－チケット返送

特表２００３－５０１７１２

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/14915

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :H04L 9/00
US CL : 713/176,181; 705/67,76, 14;
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/176,178, 179, 181; 705/1, 5, 14, 67,76, 79;

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
STN search terms: (electron? or digit?) in proximity to ((notar?) or ((contact?) in proximity to (sign?))) : ticket, coupon, timestamp

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,855,007 A (JOVICIC et al.) 29 December 1998, see entire document	1-55
Y	US RE 34,954 A (HABER et al.) 30 May 1995 - entire document, see abstract	1-55
Y	US 5,136,646 A (HABER et al.) 04 August 1992 - Abstract and entire document	1-55
A	EP 0 917 119 A2 (PALTHENGE et al.) 19 May 1999 - See Figure 9 and column 16	1-55
Y	US 5,673,320 A (RAY et al.) 30 September 1997 - entire document, see Abstract	1-55

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
18 AUGUST 2000

Date of mailing of the international search report
18 SEP 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
PINCHUS M. LAUFER
Telephone No. (703) 306-4160

Form PCT/ISA/210 (second sheet) (July 1998)*

フロントページの続き

(81)指定国　　EP (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), EA (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW